ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сведения о сертификате ЭП
Сертификат: 1ea208e57bd5c15d3d0fdd330db1ae60
Владелец: Соколов Максим Александрович
Действителен: с 06.08.2026 по 30.10.2027

УТВЕРЖДЕНО:
Ученым советом Института сервисных технологий
Протокол №24 от «16» января 2025 г.

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ
ОП.В.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена

по специальности: ***09.02.07 Информационные системы и программирование***

Квалификация: ***Специалист по информационным системам***

год начала подготовки: 2025

Разработчики:

должность	ученая степень и звание, ФИО
преподаватель	***Ашырглыжов Е.Х***

Рабочая программа согласована и одобрена руководителем ППССЗ:

должность	ученая степень и звание, ФИО
преподаватель	***Границына М.С.***

СОДЕРЖАНИЕ

1 Общая характеристика рабочей программы дисциплины

2 Структура и содержание учебной дисциплины

3 Методические указания по проведению практических занятий/лабораторных работ/семинаров, занятий в форме практической подготовки (при наличии), и самостоятельной работе

4 Фонд оценочных средств дисциплины

5 Условия реализации программы дисциплины

6 Информационное обеспечение реализации программы

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ «Информационная безопасность»

1.1 Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина «Информационная безопасность» является вариативной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.07 Информационные системы и программирование.

1.2 Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Осваиваемые компетенции

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках

В результате освоения дисциплины обучающийся должен уметь:

- применять методы и системы защиты информации;
- обеспечивать защиту и сохранность данных в сети,
- своевременно реагировать на вирусные угрозы и кибератаки
- принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации;
- администрировать подсистемы информационной безопасности различных объектов информатизации;

В результате освоения дисциплины обучающийся должен знать:

- сущность, цели и принципы информационной безопасности, законодательные основы ее реализации;
- информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности;
- направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;
- методику защиты информации в деятельности организации
- функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов.

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы учебной дисциплины	88
в т.ч. в форме практической подготовки (если предусмотрено)	-
в т. ч.:	
теоретическое обучение	34
практические и лабораторные занятия *(если предусмотрено)*	36
Самостоятельная работа	4
Консультации	2
Промежуточная аттестация (Экзамен в 6 семестре)	12

2.2. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, Практические работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Тема 1. Концепции и аспекты обеспечения информационной безопасности	**Лекционные занятия:**		
	1. Понятия экономической и информационной безопасности. 2. Ключевые вопросы информационной безопасности	**6**	
Тема 2. Виды угроз информационной безопасности	**Лекционные занятия:**		
	3. Виды угроз информационной безопасности 4. Основные виды защищаемой информации	**6**	
	Практическое занятие 1		
	Основы законодательства в области обеспечения информационной безопасности	8	
	Разработка метода и модели системы защиты информации.		
	Алгоритм проведения анализа и оценки угроз.		
Тема 3. Построения системы информационной безопасности	**Лекционные занятия:**	**6**	
	5. Основные аспекты построения системы информационной безопасности 6. Анализ и управление рисками при реализации информационной безопасности		
	Практическое занятие 2	6	
	Адаптивная модель СЗИ на базе нейронных сетей.		

	Схема работы генетического алгоритма		
Тема 4. Защита информации в информационных системах и компьютерных сетях	**Лекционные занятия:**	**6**	
	7. Защита информации в информационных системах и компьютерных сетях.		
	8. Методология анализа защищенности информационной системы.		
	Практическое занятие 3 Трёхуровневая модель параметров оценки защищенности ИС. Модели системы защиты.	6	
Тема 5. Обеспечение безопасности ИС	**Лекционные занятия:**	**6**	
	9. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. 10. Технологии криптографической защиты информации. Современные средства биометрической идентификации.		
	Практическое занятие 4 Защита информации в распределенной ИС. Шифрование и дешифрование данных. Таблица Вижинера	8	
Тема 6. Обеспечение интегральной безопасности ИС	**Лекционные занятия:**	**4**	
	11. Обеспечение интегральной безопасности информационных систем и сетей 12. Технологии криптографической защиты информации.		
	Практическое занятие 5 Распределенная информационная система. Технологии токенов Компоновка VPN на основе международных стандартов и протоколов.	8	
	Самостоятельная работа 5 Систематическая проработка конспектов занятий, учебной и специальной технической литературы по темам:	4	

	Принципы организации разноуровневого доступа в автоматизированных информационных системах. Понятие несанкционированного доступа и защита от него. Управление доступом в информационных системах. Основные понятия: клиент, право и объект доступа, группы, роли, политика безопасности. Дискреционная модель доступа. Преимущества и недостатки. Мандатная модель доступа. Преимущества и недостатки.		
Консультации		**2**	
Промежуточная аттестация (экзамен в 6 семестре)		**12**	
Всего		**88**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. Методические указания по проведению практических занятий/лабораторных работ/семинаров, занятий в форме практической подготовки (при наличии), и самостоятельной работе

Практические занятия заключаются в выполнении студентами, под руководством преподавателя, комплекса учебных заданий направленных на усвоение научно-теоретических основ учебной дисциплины, приобретение практических навыков овладения методами практической работы с применением современных средств компьютерной графики, мультимедиа, коммуникационных технологий.

Практические занятия способствуют более глубокому пониманию теоретического материала учебного курса, а также развитию, формированию и становлению различных уровней составляющих профессиональной компетентности студентов. Наряду с формированием умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать эти навыки на практике, развиваются интеллектуальные умения.

Практические занятия проводятся в форме практических работ.

3.1. Тематика и содержание практических занятий

Тема 2. Виды угроз информационной безопасности
Практическое занятие 1.
«Основы законодательства в области обеспечения информационной безопасности».
Практическое занятие 2.
«Разработка метода и модели системы защиты информации».
Практическое занятие 3.
«Алгоритм проведения анализа и оценки угроз».
Тема 3. Построения системы информационной безопасности
Практическое занятие 1.
«Адаптивная модель СЗИ на базе нейронных сетей».
Практическое занятие 2.
«Схема работы генетического алгоритма».
Тема 4. Защита информации в информационных системах и компьютерных сетях
Практическое занятие 1.
«Адаптивная модель СЗИ на базе нейронных сетей».
Практическое занятие 2.
«Схема работы генетического алгоритма».
Тема 5. Обеспечение безопасности ИС
Практическое занятие 1.
«Защита информации в распределенной ИС».
Практическое занятие 2.
«Шифрование и дешифрование данных. Таблица Вижинера».
Тема 6. Обеспечение интегральной безопасности ИС
Практическое занятие 1.
«Распределенная информационная система».
Практическое занятие 2.
«Технологии токенов».
Практическое занятие 3.
«Компоновка VPN на основе международных стандартов и протоколов».

3.2. Тематика и содержание самостоятельной работы

Самостоятельная работа является неотъемлемой частью образовательного процесса, связанного с формированием компетенций обучающихся.

Целью самостоятельной (внеаудиторной) работы студентов является обучение навыкам работы с научно-теоретической, периодической, научно-технической литературой и технической документацией, необходимыми для углубленного изучения дисциплины, а также развитие у них устойчивых способностей к самостоятельному изучению и изложению полученной информации.

Формы (виды) самостоятельной работы

Самостоятельная работа выполняется в форме проработки конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) и подготовки к практическим работам с использованием методических рекомендаций преподавателя; оформление практических работ; отчетов и подготовка к их защите.

Тематика и содержание

Примерные темы докладов

1) Основные термины и определения безопасности и защиты информации

2) Сущность и понятие информационной безопасности и защиты информации

3) Цели и концептуальные основы информационной безопасности и защиты информации

4) Принцип историчности в системах безопасности и защиты информации

5) Конфиденциальная информация. Классификация по видам и степеням конфиденциальности

6) Носители защищаемой информации

7) Потенциальные угрозы защищаемой информации. Виды и методы дестабилизирующего воздействия на защищаемую информацию.

8) Элементарная и многозвенная модель защиты информации

9) Модель многоуровневой защиты

10) Комплексная вероятностная модель защиты информации

11) Расчет надежности защиты информации

12) Законодательные средства защиты информации

13) Организационно-законодательные средства защиты информации

14) Физические средства защиты информации

15) Аппаратные средства защиты информации

16) Программные и криптографические средства защиты информации

17) Порядок определения комплекса средств защиты информации для объекта информатизации

18) Основные положения криптографии. Теоретическая и практическая стойкость шифров. Допущения Шеннона

19) Методы криптографического преобразования данных. Перестановка.

20) Методы криптографического преобразования данных. Гаммирование.

21) Методы криптографического преобразования данных. Аналитические преобразования.

22) Основные положения построения симметричных и несимметричных криптосистем

23) Однонаправленные функции

24) Практическое применение шифров. Таблица Вижинера.

25) Практическое применение шифров. Таблица Метод RSA.

26) Виды и сущность криптоанализа. Правило Киркхоффа

27) Понятие и основные положения цифровой стеганографии

28) Принципы организации разноуровневого доступа в автоматизированных информационных системах.

29) Понятие несанкционированного доступа и защита от него.

30) Управление доступом в информационных системах. Основные понятия: клиент, право и объект доступа, группы, роли, политика безопасности.

31) Дискреционная модель доступа. Преимущества и недостатки.

32) Мандатная модель доступа. Преимущества и недостатки.

33) Сущность и проявление РПС (компьютерных вирусов).

34) Классификация компьютерных вирусов.

35) Основные виды вирусов и схемы их функционирования.

36) Программы обнаружения и защиты от вирусов, особенности их работы.

4. Фонд оценочных средств дисциплины

4.1. Результаты освоения учебной дисциплины, подлежащие проверке

Формы промежуточной аттестации по семестрам:

№ семестра	Форма контроля
6	Экзамен

В результате промежуточной аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний:

Результаты обучения: умения, знания и общие компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Умения		
У1. применять методы и системы защиты информации;	Правильное и адекватное применение методов и систем защиты информации.	*Для текущего контроля:* оценка результатов практических занятий; *Для промежуточной аттестации:* экзамен
У2. обеспечивать защиту и сохранность данных в сети;	Обеспечение защиты и сохранности данных в сети.	*Для текущего контроля:* оценка результатов практических занятий; *Для промежуточной аттестации:* экзамен
У3. своевременно реагировать на вирусные угрозы и кибератаки;	Знание современных систем защиты.	*Для текущего контроля:* оценка результатов практических занятий;

		Для промежуточной аттестации: экзамен
У4. принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации;	Эксплуатация подсистем управления информацион-ной безопасностью различных объектов информатизации	*Для текущего контроля:* оценка результатов практических занятий; *Для промежуточной аттестации:* экзамен
У5. администрировать подсистемы информационной безопасности различных объектов информатизации.	Умение администрировать подсистемы информационной безопасности различных объектов информатизации	*Для текущего контроля:* оценка результатов практических занятий; *Для промежуточной аттестации:* экзамен
Знания		
З1. сущность, цели и принципы информационной безопасности, законодательные основы ее реализации;	- активное использование различных источников для решения профессиональных задач;	*Для текущего контроля:* устный опрос. *Для промежуточной аттестации:* экзамен
З2. информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности;	- освоение информации и программ, необходимых для профессиональной деятельности;	*Для текущего контроля:* устный опрос. *Для промежуточной аттестации:* экзамен
З3. направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;	- активное использование в учебной деятельности информационных и коммуникационных ресурсов;	*Для текущего контроля:* устный опрос. *Для промежуточной аттестации:* экзамен
З4. методику защиты информации в деятельности организации;	- освоение программ, необходимых для профессиональной деятельности;	*Для текущего контроля:* устный опрос. *Для промежуточной аттестации:* экзамен
З5. функциональные возможности и предпосылки	- соответствие способов достижения цели, способам определенным	*Для текущего контроля:* устный опрос. *Для промежуточной аттестации:*

эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов;	руководителем и документами;	экзамен

Формируемые компетенции:

Код формируемой компетенции	**Наименование компетенции**	**Формы и методы контроля и оценки результатов обучения**
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 4.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях;	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен

	учетом особенностей социального и культурного контекста.	
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языке.	*Для текущего контроля:* оценка результатов практических занятий, устный опрос. *Для промежуточной аттестации:* экзамен

4.2. Методика применения контрольно-измерительных материалов

Контроль знаний обучающихся включает:

- Текущий контроль проходит в форме тестирования
- Промежуточную аттестацию проходит в форме экзамена

4.3. Контрольно-измерительные материалы включают:

4.3.1. Типовые задания для оценки знаний и умений текущего контроля

Контроль и оценка результатов освоения темы осуществляется преподавателем в процессе выполнения обучающимися индивидуальных заданий **в виде тестовых заданий, практических работ, устного опроса.**

Тестовые задания

ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

Задания закрытого типа на установление соответствия

Задание 1

Установите соответствие между типами угроз информационной безопасности и способами их предотвращения:

a) Фишинг	а) Установка антивирусного программного обеспечения
b) DDoS-атака	б) Обучение сотрудников правилам кибергигиены
c) Утечка данных	в) Настройка систем мониторинга сетевого трафика
d) Вредоносное ПО	г) Шифрование конфиденциальных данных

Задание 2

Установите соответствие между этапами обработки инцидентов информационной безопасности и действиями:

a) Идентификация инцидента	а) Определение источника атаки
b) Анализ инцидента	б) Восстановление данных из резервных копий
c) Устранение последствий	в) Обновление политик безопасности
d) Профилактика	г) Обнаружение аномальной активности в сети

Задания закрытого типа на установление последовательности

Задание 1
Установите правильную последовательность действий при реагировании на утечку данных:

a) Блокировка доступа к compromised-системам
b) Сбор и анализ данных об инциденте
c) Уведомление заинтересованных сторон
d) Восстановление данных и систем
e) Проведение аудита безопасности

Задание 2
Установите правильную последовательность этапов разработки политики информационной безопасности:

a) Анализ рисков
b) Определение целей и задач политики
c) Разработка мер защиты
d) Внедрение политики
e) Обучение сотрудников

Задания комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Задание 1
Какой из перечисленных методов является наиболее эффективным для предотвращения атак социальной инженерии?

а) Установка антивируса
б) Регулярное обучение сотрудников
в) Использование сложных паролей
г) Настройка брандмауэра

Задание 2
Какой из перечисленных способов наиболее эффективен для защиты от DDoS-атак?

а) Использование CAPTCHA
б) Настройка систем фильтрации трафика
в) Шифрование данных
г) Регулярное обновление ПО

Задания комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Задание 1
Какие из перечисленных мер помогут предотвратить утечку конфиденциальных данных? (Выберите несколько вариантов)

а) Шифрование данных
б) Регулярное резервное копирование
в) Ограничение доступа к данным
г) Использование VPN

Задание 2
Какие из перечисленных действий необходимы для обеспечения безопасности мобильных устройств? (Выберите несколько вариантов)

а) Установка антивирусного ПО
б) Регулярное обновление ОС
в) Использование публичных Wi-Fi сетей
г) Настройка двухфакторной аутентификации

Задания открытого типа с развернутым ответом

Задание 1
Опишите, какие меры необходимо предпринять для защиты корпоративной сети от атак типа "человек посередине" (Man-in-the-Middle). Укажите не менее трех мер и обоснуйте их эффективность.

Задание 2
Предложите план действий для организации в случае обнаружения утечки конфиденциальных данных. Включите этапы от идентификации инцидента до профилактики повторных случаев.

ОК 2.Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

Задания закрытого типа на установление соответствия

Задание 1
Установите соответствие между инструментами анализа данных и их назначением:

1. SIEM-системы
2. Сканеры уязвимостей
3. Сетевые анализаторы
4. Программы для анализа журналов

а) Обнаружение уязвимостей в сетевых устройствах
б) Мониторинг и анализ событий безопасности в реальном времени
в) Анализ сетевого трафика
г) Обработка и интерпретация лог-файлов

Задание 2
Установите соответствие между этапами анализа данных и инструментами, которые используются на каждом этапе:

1. Сбор данных
2. Обработка данных
3. Анализ данных
4. Визуализация результатов

а) Программы для построения графиков и диаграмм
б) Сетевые анализаторы (например, Wireshark)
в) Инструменты для машинного обучения (например, Python, R)
г) Базы данных и системы хранения логов

Задания закрытого типа на установление последовательности

Задание 1
Установите правильную последовательность этапов анализа сетевого трафика:

a) Сбор сетевого трафика
b) Фильтрация данных
c) Анализ пакетов
d) Интерпретация результатов
e) Составление отчета

Задание 2
Установите правильную последовательность этапов работы с SIEM-системой:

a) Настройка правил корреляции
b) Сбор данных с источников
c) Анализ событий безопасности
d) Генерация отчетов
e) Реагирование на инциденты

Задания комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Задание 1
Какой инструмент наиболее эффективен для анализа сетевого трафика в реальном времени?

а) Wireshark
б) Nmap
в) Metasploit
г) Nessus

Задание 2
Какой из перечисленных инструментов используется для автоматизации сбора и анализа логов?

а) Splunk
б) Nmap

в) Burp Suite
г) John the Ripper

Задания комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Задание 1
Какие из перечисленных инструментов используются для анализа уязвимостей? (Выберите несколько вариантов)

а) Nessus
б) Wireshark
в) OpenVAS
г) Metasploit

Задание 2
Какие из перечисленных инструментов подходят для анализа журналов событий? (Выберите несколько вариантов)

а) Splunk
б) ELK Stack (Elasticsearch, Logstash, Kibana)
в) Nmap
г) Burp Suite

Задания открытого типа с развернутым ответом

Задание 1
Опишите, как можно использовать SIEM-систему для выявления аномальной активности в корпоративной сети. Укажите этапы работы и примеры анализируемых данных.

Задание 2
Предложите план использования инструментов анализа данных для расследования инцидента, связанного с утечкой информации. Укажите, какие инструменты и методы будут использоваться на каждом этапе.

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде

Задания закрытого типа на установление соответствия

Задание 1

Установите соответствие между этапами профессионального развития и действиями:

1. Постановка целей
2. Планирование
3. Реализация

4. Оценка результатов

а) Составление плана обучения и развития
б) Анализ достигнутых результатов и корректировка планов
в) Определение карьерных и личных целей
г) Выполнение запланированных действий

Задание 2

Установите соответствие между понятиями финансовой грамотности и их описанием:

1. Бюджетирование
2. Инвестирование
3. Страхование
4. Кредитование

а) Распределение доходов и расходов
б) Вложение средств с целью получения дохода
в) Защита от финансовых рисков
г) Получение заемных средств

Задания закрытого типа на установление последовательности

Задание 1

Установите правильную последовательность этапов создания бизнес-плана:

1. Анализ рынка
2. Постановка целей
3. Разработка финансового плана
4. Реализация проекта
5. Оценка результатов

Задание 2

Установите правильную последовательность этапов личного финансового планирования:

a) Определение финансовых целей
b) Анализ доходов и расходов
c) Создание бюджета
d) Инвестирование сбережений
e) Регулярный мониторинг и корректировка

Задания комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Задание 1

Какой из перечисленных инструментов наиболее эффективен для планирования личного бюджета?

а) Таблицы Excel
б) Мобильные приложения для учета финансов
в) Бумажный блокнот
г) Калькулятор

Задание 2

Какой из перечисленных способов наиболее эффективен для снижения финансовых рисков?

а) Инвестирование в акции
б) Страхование имущества
в) Покупка криптовалюты
г) Хранение денег дома

Задания комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Задание 1

Какие из перечисленных действий способствуют профессиональному развитию? (Выберите несколько вариантов)

а) Посещение курсов повышения квалификации
б) Чтение профессиональной литературы
в) Участие в конференциях
г) Игнорирование новых технологий

Задание 2

Какие из перечисленных действий помогут улучшить финансовую грамотность? (Выберите несколько вариантов)

а) Изучение основ инвестирования
б) Составление личного бюджета
в) Игнорирование финансовых новостей
г) Использование кредитов без анализа условий

Задания открытого типа с развернутым ответом

Задание 1

Опишите, как вы планируете свое профессиональное развитие в области информационной безопасности на ближайшие 5 лет. Укажите конкретные шаги и ресурсы.

Задание 2

Предложите план действий для создания собственного бизнеса в сфере информационной безопасности. Укажите ключевые этапы и ресурсы.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

Задания закрытого типа на установление соответствия

Задание 1

Установите соответствие между видами коммуникации и их характеристиками:

1. Устная коммуникация
2. Письменная коммуникация
3. Невербальная коммуникация
4. Официальная коммуникация

а) Использование жестов и мимики
б) Проведение презентаций и выступлений
в) Написание отчетов и писем
г) Соблюдение норм делового этикета

Задание 2

Установите соответствие между элементами делового письма и их описанием:

1. Заголовок
2. Основной текст
3. Подпись
4. Приложение

а) Содержит основную информацию
б) Указывает на наличие дополнительных материалов
в) Включает имя и должность отправителя
г) Отражает тему письма

Задания закрытого типа на установление последовательности

Задание 1

Установите правильную последовательность этапов подготовки к публичному выступлению:

a) Определение цели выступления
b) Сбор информации
c) Составление плана выступления
d) Репетиция
e) Выступление

Задание 2

Установите правильную последовательность написания делового письма:

a) Формулировка темы
b) Написание основного текста
c) Проверка орфографии и стиля
d) Добавление подписи
e) Отправка письма

Задания комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Задание 1

Какой из перечисленных элементов наиболее важен для успешной устной коммуникации?

а) Грамотная речь
б) Использование сложных терминов
в) Минимальный зрительный контакт
г) Отсутствие пауз

Задание 2

Какой из перечисленных стилей наиболее подходит для написания делового письма?

а) Официально-деловой
б) Разговорный
в) Художественный
г) Научный

Задания комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Задание 1

Какие из перечисленных элементов должны быть включены в деловое письмо? (Выберите несколько вариантов)

а) Заголовок
б) Основной текст
в) Подпись
г) Смайлики

Задание 2

Какие из перечисленных действий способствуют эффективной устной коммуникации? (Выберите несколько вариантов)

а) Поддержание зрительного контакта
б) Использование профессионального жаргона
в) Четкое произношение слов
г) Отсутствие пауз

Задания открытого типа с развернутым ответом

Задание 1

Опишите, как вы подготовитесь к публичному выступлению на конференции по информационной безопасности. Укажите ключевые этапы.

Задание 2

Напишите пример делового письма с запросом на предоставление информации о новых технологиях в области информационной безопасности.

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

Задания закрытого типа на установление соответствия

Задание 1

Установите соответствие между принципами бережливого производства и их описанием:

1. Устранение потерь	а) Поиск и устранение неэффективных процессов
2. Постоянное улучшение	б) Вовлечение сотрудников в улучшение процессов
3. Уважение к людям	в) Ориентация на потребности клиента
4. Создание ценности	г) Снижение затрат и повышение качества

Задание 2

Установите соответствие между действиями и их влиянием на окружающую среду:

1. Использование энергосберегающих технологий
2. Переработка отходов
3. Сокращение использования бумаги
4. Участие в экологических акциях

а) Снижение выбросов углекислого газа
б) Уменьшение объема мусора на свалках
в) Сохранение лесных ресурсов
г) Повышение экологической осведомленности

Задания закрытого типа на установление последовательности

Задание 1

Установите правильную последовательность действий при возникновении чрезвычайной ситуации:

a) Оценка ситуации
b) Оповещение сотрудников
c) Эвакуация
d) Ликвидация последствий
e) Анализ и предотвращение

Задание 2

Установите правильную последовательность этапов внедрения принципов бережливого производства:

a) Анализ текущих процессов
b) Выявление потерь
c) Разработка улучшений
d) Внедрение изменений
e) Оценка результатов

Задания комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Задание 1

Какой из перечисленных способов наиболее эффективен для снижения энергопотребления в офисе?

а) Использование энергосберегающих ламп
б) Увеличение количества техники

в) Отключение систем отопления
г) Установка дополнительных кондиционеров

Задание 2

Какой из перечисленных принципов наиболее важен для бережливого производства?

а) Устранение потерь
б) Увеличение запасов
в) Увеличение времени производства
г) Сокращение числа сотрудников

Задания комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Задание 1

Какие из перечисленных действий способствуют ресурсосбережению? (Выберите несколько вариантов)

а) Использование перерабатываемых материалов
б) Увеличение потребления воды
в) Сокращение использования бумаги
г) Утилизация отходов

Задание 2

Какие из перечисленных действий помогут снизить воздействие на климат? (Выберите несколько вариантов)

а) Использование возобновляемых источников энергии
б) Увеличение выбросов углекислого газа
в) Сокращение использования пластика
г) Участие в программах по озеленению

Задания открытого типа с развернутым ответом

Задание 1

Опишите, как можно внедрить принципы бережливого производства в компании, занимающейся информационной безопасностью. Укажите конкретные шаги.

Задание 2

Предложите план действий для снижения энергопотребления в офисе компании. Укажите ключевые меры.

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языке.

Задания закрытого типа на установление соответствия

Задание 1

Установите соответствие между видами профессиональной документации и их описанием:

1. Технические стандарты
2. Руководства пользователя
3. Регламенты
4. Отчеты

а) Описание правил и процедур
б) Инструкции по использованию оборудования
в) Документы, содержащие результаты работы
г) Нормативные документы, устанавливающие требования

Задание 2

Установите соответствие между типами документов и их назначением:

1. Политика безопасности
2. Инструкция по эксплуатации
3. Техническое задание
4. Акт проверки

а) Описание требований к системе безопасности
б) Руководство по использованию оборудования
в) Документ, фиксирующий результаты проверки
г) Описание задач и требований к проекту

Задания закрытого типа на установление последовательности

Задание 1

Установите правильную последовательность этапов работы с технической документацией:

a) Изучение документации
b) Анализ требований
c) Применение на практике
d) Оценка результатов
e) Корректировка документации

Задание 2

Установите правильную последовательность этапов перевода профессиональной документации:

a) Чтение и понимание исходного текста
b) Перевод текста
c) Проверка перевода на соответствие терминологии
d) Редактирование и оформление
e) Сдача перевода

Задания комбинированного типа с выбором одного верного ответа из четырех предложенных и обоснованием выбора

Задание 1

Какой из перечисленных документов является обязательным для соблюдения в области информационной безопасности?

а) Техническое задание
б) Политика безопасности
в) Руководство пользователя
г) Акт проверки

Задание 2

Какой из перечисленных языков наиболее часто используется в международной профессиональной документации по информационной безопасности?

а) Русский
б) Английский
в) Немецкий
г) Китайский

Задания комбинированного типа с выбором нескольких вариантов ответа из предложенных и развернутым обоснованием выбора

Задание 1

Какие из перечисленных документов относятся к нормативной документации в области информационной безопасности? (Выберите несколько вариантов)

а) ГОСТ Р 50922-2006
б) Руководство по настройке firewall
в) Политика безопасности организации
г) Техническое задание на разработку ПО

Задание 2

Какие из перечисленных действий необходимы для корректного перевода профессиональной документации? (Выберите несколько вариантов)

а) Использование профессиональной терминологии
б) Дословный перевод без учета контекста
в) Проверка перевода на соответствие стандартам
г) Игнорирование структуры документа

Задания открытого типа с развернутым ответом

Задание 1

Опишите, как вы будете работать с технической документацией на иностранном языке при внедрении нового программного обеспечения для защиты данных. Укажите ключевые этапы.

Задание 2

Напишите пример фрагмента технической документации на английском языке с переводом на русский язык.

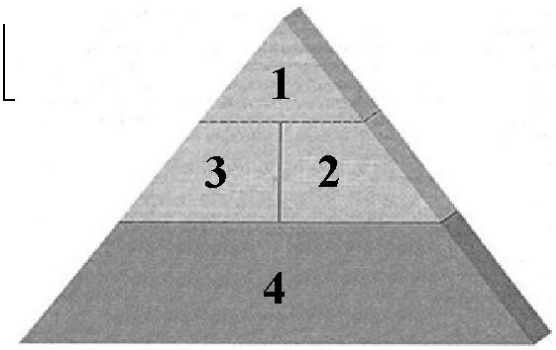
Перечень теоретических вопросов:

1 Главная цель мер, предпринимаемых на административном уровне:
2 Какие угрозы являются самыми опасными?
3 Какова главная задача мер административного уровня?
4 Какую функцию выполняет экран?
5 Меры информационной безопасности направлены на защиту от:
6 Назовите виды мер безопасности
7 Назовите главные угрозы ИБ
8 Назовите методы процедурного уровня защиты ИБ
9 Назовите самыме опасные источники внутренних угроз
10 Назовите три главные цели реакции на нарушение режима ИБ
11 Назовите четыре уровня ИБ
12 Назовите этапы жизненного цикла ИС
13 Назовите этапы процесса планирования восстановительных работ
14 Первый шаг в анализе угроз - это:
15 Перечислите принципы архитектурной безопасности
16 Перечислите сервисы безопасности программно-технического уровня
17 Принцип усиления самого слабого звена можно переформулировать как:
18 Риск является функцией:
19 С чего начинается разработка политики и программы безопасности?
20 Самыми опасными источниками угрозами являются:
21 Согласно закону "О лицензировании отдельных видов деятельности", лицензия - это:

22 Согласно закону "Об информации, информатизации и защите информации", персональные данные - это:
23 Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:
24 Цель мероприятий в области информационной безопасности
25 Чем измеряется эффективность информационного сервиса?
26 Чем хорош статистический метод выявления атак?
27 Что необходимо оценить после индефикации угрозы?
28 Что отражает политика безопасности
29 Что понимается под информационной безопасностью?
30 Что содержит цифровой сертификат?
31 Что такое защита информации?
32 Что такое программно-технические меры?

4.3.2. Типовые задания для оценки знаний и умений промежуточной аттестации

Перечень тем для проведения экзамена
по «Информационной безопасности»

Тема 1. Концепции и аспекты обеспечения информационной безопасности	
1	**Какие компоненты и в каком порядке входят в общую структуру ИБ?**
	Борьба с вредоносным ПО
	Инфраструктура безопасности
	Криптографическая защита
	Управление рисками
	Управление угрозами
	Управление уязвимостями
	
2	**Состав инфраструктуры безопасности**
	Антивирусная защита
	Идентификация и аутентификация
	Криптографическая защита
	Разграничение доступа

	Управление угрозами
	Управление уязвимостями
3	**Требования по обеспечению безопасности в различных аспектах информационной деятельности всегда направлены на достижение следующих трёх основных составляющих информационной безопасности:**
	Доступность
	Защищенность
	Конфиденциальность
	Неуязвимость
	Целостность
4	**Деятельность по обеспечению информационной безопасности направлена на то, чтобы не допустить, предотвратить или нейтрализовать:**
	искажение, частичную или полную утрату конфиденциальной информации;
	невыполнение плана продаж
	несанкционированный доступ к информационным ресурсам (НСД, Unauthorized Access — UAA);
	неэффективную работу персонала
	отказы и сбои в работе программно-аппаратного и телекоммуникационного обеспечения.
	целенаправленные действия (атаки) по разрушению целостности программных комплексов, систем данных и информационных структур;
5	**Ключевые вопросы информационной безопасности**
	во что обойдется разработка, внедрение, эксплуатация, сопровождение и развитие систем защиты?
	как надо защищаться?
	когда надо защищаться?
	надо ли защищаться и что следует защищать?
	от кого надо защищаться?
	от чего надо защищаться?
	почему надо защищаться?
	что обеспечит эффективность защиты?
6	**Система ИБ включает необходимый комплекс мероприятий и технических решений по защите:**
	от внедрения новых корпоративных информационных систем
	от внедрения программных "вирусов" и "закладок" в программные продукты и технические средства.

	от нарушения функционирования информационного пространства путем исключения воздействия на информационные каналы и ресурсы;
	от несанкционированного доступа к информации путем обнаружения и ликвидации попыток использования ресурсов информационного пространства, приводящих к нарушению его целостности;
	от погодных условий
	от разрушения встраиваемых средств защиты с возможностью доказательства неправомочности действий пользователей и обслуживающего персонала;
7	**Ранжируйте ИТ-угрозы по степени опасности**
	Аппаратные и программные сбои
	Вредоносные программы
	Действия инсайдеров
	Кража оборудования
	Спам
	Финансовое мошенничество
	Хакерские атаки
	Халатность сотрудников
8	**Добавьте недостающие заимосвязанные параметры поля информационной безопасности**
	Атаки
	Риски
	Уязвимости
	

9	**Расставьте по порядку составляющие инфраструктуры информационной безопасности**
	Единственность точки входа
	Конфиденциальность
	Целостность приложений/данных
	Целостность сети
	Целостность системы
Тема 2. Виды угроз информационной безопасности	
1	**Цепочка анализа проблем ИБ с учетом взаимосвязи экономических противоречий, угроз и потерь, к которым может приводить реализация угроз.**
	возможность её реализации (предпосылки, объект, способ действия, скорость и временной интервал действия)
	зона риска (сфера экономической деятельности предприятия, способы её реализации, материальные и информационные ресурсы)
	источник угрозы (внешняя и/или внутренняя среда предприятия)
	последствия (материальный ущерб, моральный вред, размер ущерба и вреда, возможность компенсации)
	угроза (вид, величина, направление)
	фактор (степень уязвимости данных, информации, программного обеспечения, компьютерных и телекоммуникационных устройств, материальных и финансовых ресурсов, персонала)
2	**Критерии классификации угроз**
	по важнейшим составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых направлены угрозы в первую очередь;
	по квалификации злоумышленников

	по компонентам информационных систем и технологий (данные, программно-аппаратные комплексы, сети, поддерживающая инфраструктура), на которые угрозы непосредственно нацелены;
	по локализации источника угроз (вне или внутри информационной технологии или системы).
	по способу осуществления (случайные или преднамеренные действия, события техногенного или природного масштаба);
	по стоимости нанесенного ущерба
3	**Обычно пользователи могут быть источниками следующих угроз:**
	случайная
	намеренная (встраивание логической бомбы, которая со временем разрушит программное ядро или приложения) или непреднамеренная потеря или искажение данных и информации, "взлом" системы администрирования, кража данных и паролей, передача их посторонним лицам и т.д.;
	невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т. п.).
	нежелание пользователя работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности или при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками) и намеренный вывод из строя её программно-аппаратных устройств;
	религиозные убеждения
4	**Набор политик по реализации внутренней информационной безопасности:**
	политика информационной безопасности;
	политика использования Internet/Intranet;
	политика использования электронной почты;
	политика предоставления прав доступа к внутренним и удаленным ресурсам;
	порядок инвентаризации информационных ресурсов;
	порядок приема на работу новых сотрудников
	правила противопожарной безопасности
	соглашение о неразглашении данных и информации, составляющих коммерческую тайну и имеющих грифы "конфиденциально" и "для служебного пользования".

Тема 3. Построения системы информационной безопасности	
1	**Программа ИБ должна содержать следующие главные цели:**
	контроль деятельности в области ИБ
	координация деятельности в области информационной безопасности: выбор эффективных средств защиты, их приобретение или разработка, внедрение, эксплуатация, пополнение и распределение ресурсов, обучение персонала
	оценка рисков и управление рисками
	повышение эффективности работы подразделений и пользователей
	разработку и исполнение политики в области ИБ
	снижение накладных расходов
	стратегическое планирование в области развития информационной безопасности
2	**При построении теоретических моделей систем защиты информации (СЗИ) и информационных ресурсов необходимо опираться на следующие важнейшие обстоятельства:**
	выбор математически строгих критериев для оценки оптимальности системы защиты информации для данной архитектуры ИС;
	четкая математическая формулировка задачи построения модели СЗИ, учитывающая заданные требования к системе защиты и позволяющая построить СЗИ в соответствии с этими критериями.
	правовые и законодательные нормы
	технические характеристики оборудования
3	**Типичные вопросы при следовании политики безопасности нижнего уровня:**
	как организован удаленный доступ к сервису?
	как построена локальная сеть предприятия?
	кто имеет право доступа к объектам, поддерживаемым сервисом?
	кто имеет право модернизировать сервис?
	кто руководит сервисом?
	при каких условиях можно читать и модифицировать данные?
4	**При оценке уровня рисков как "оправданный" используются следующие типы контрмер по снижению уровня потерь:**
	Передача
	Принятие
	Смягчение

	Уклонение
5	**В итерационном процессе управления рисками этап Администрирование состоит из следующих пунктов**
	Аудит системы управления
	Реализация программы управления рисками
	Ресурсы
	Структура, связи и ответственность
	Управление документацией
Тема 4. Защита информации в информационных системах и компьютерных сетях	
1	**Можно выделить ряд особенностей, которые делают сети уязвимыми, а нарушителей — практически неуловимыми:**
	возможность действия нарушителей на расстоянии в сочетании с возможностью сокрытия своих истинных персональных данных
	возможность многократного повторения атакующих сеть воздействий
	возможность пропаганды и распространения средств нарушения сетевой безопасности
	высокая скорость интернет-соединения
	техническая эволюция мобильных устройств
2	**Оценка уровня защищенности ИТ/ИС обычно производится по следующим базовым группам критериев**
	Безопасность
	Безотказность
	Исполнение
	Система целей
	Средства
3	**Существуют следующие модели системы защиты**
	абсолютно неуязвимая
	абсолютно уязвимая
	с полным перекрытием
	содержащая уязвимости
Тема 5. Обеспечение безопасности ИС	
1	**Анализ безопасности ИС при отсутствии злоумышленных факторов базируется на модели взаимодействия основных компонент ИС. В качестве объектов уязвимости рассматриваются:**
	данные и информация, накопленная в базах данных;

	динамический вычислительный процесс обработки данных, автоматизированной подготовки решений и выработки управляющих воздействий;
	жесткие диски персональных компьютеров
	информация, выдаваемая потребителям и на исполнительные механизмы.
	локальные вычислительные сети
	объектный код программ, исполняемых вычислительными средствами в процессе функционирования ИС;
2	**Внутренними дестабилизирующими факторами и угрозами безопасности системы при отсутствии злоумышленных угроз являются**
	Искажения информации в каналах
	Недостаточное качество средств защиты
	Ошибки алгоритмизации задач
	Ошибки персонала при эксплуатации
	Ошибки программирования
	Ошибки проектирования при постановке задач
3	**Внешними дестабилизирующими факторами и угрозами безопасности системы при отсутствии злоумышленных угроз являются**
	Изменения конфигурации системы
	Искажения информации в каналах
	Недостаточное качество средств защиты
	Ошибки персонала при эксплуатации
	Ошибки программирования
	Сбои и отказы аппаратуры
4	**Критериями адекватности средств защиты являются:**
	Критерии быстродействия
	Критерии защищенности
	Критерии корректности
	Критерии эффективности
5	**Технологии криптографии позволяют реализовать следующие процессы информационной защиты:**
	аутентификация (проверка подлинности) объекта или субъекта сети
	доступность интернет-сервисов
	идентификация (отождествление) объекта или субъекта сети или информационной системы
	контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам

	обеспечение и контроль целостности данных.
	обеспечение электробезопасности объектов сети
6	**Функциональные возможности межсетевых экранов охватывают следующие разделы реализации информационной безопасности:**
	администрирование доступа во внутренние сети
	ведение журналов и учет
	информационную поддержку пользователей
	настройку правил фильтрации
	средства сетевой аутентификации
	фильтрацию на прикладном уровне
	фильтрацию на сетевом уровне
	электронный документооборот
7	**По схеме подключения межсетевые экраны можно разделить на:**
	схема "звезда"
	схема "кольцо"
	схема единой защиты сети
	схема с закрытым и не защищаемым открытым сегментами сети
	схема с раздельной защитой закрытого и открытого сегментов сети
Тема 6. Обеспечение интегральной безопасности ИС	
1	**Три основных подхода осуществления информационной безопасности:**
	Интегральный
	Комплексный
	Финансовый
	Частный
	Эффективный
2	**Основным элементом электронного ключа-жетона (токена) является**
	микроконтроллер
	программное обеспечение
	интерфейс
	контактные площадки
3	**Интегральная безопасность информационных систем включает в себя следующие составляющие:**
	безопасность данных — обеспечение конфиденциальности, целостности и доступности данных.

	безопасность сетей и телекоммуникационных устройств — защита каналов связи от воздействий любого рода;
	безопасность системного и прикладного программного обеспечения — защита от вирусов, логических "мин", несанкционированного изменения конфигурации систем и программного кода;
	интеллектуальная безопасность - защита авторских и смежных прав на ПО
	физическая безопасность — защита зданий, помещений, подвижных средств, людей, а также аппаратных средств (компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
4	**Расположите современные электронные средства, используемых для контроля доступа, по порядку роста эффективности**
	Биометрия
	Карты и жетоны
	Код + карта
	Код + карта + биометрия
	Кодовый замок

Тестовые задания:

1.	К негативным последствиям развития современных информационных и коммуникационных технологий можно отнести:	
	А)	формирование единого информационного пространства
	Б)	работа с информацией становится главным содержанием профессиональной деятельности
	В)	организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации
	Г)	широкое использование информационных технологий во всех сферах человеческой деятельности
	Д)	доступность личной информации для общества и государства, вторжение информационных технологий в частную жизнь людей
2.	Термин «информатизация общества» обозначает:	
	А)	целенаправленное и эффективное использование информации во всех областях человеческой деятельности на основе современных информационных и коммуникационных технологий
	Б)	увеличение избыточной информации, циркулирующей в обществе
	В)	увеличение роли средств массовой информации
	Г)	введение изучения информатики во все учебные заведения страны
	Д)	организацию свободного доступа каждого человека к информационным ресурсам человеческой цивилизации
3.	Развитый рынок информационных продуктов и услуг, изменение в структуре	

	экономики, массовое использование информационных и коммуникационных технологий являются признаками:	
	А)	информационной культуры
	Б)	высшей степени развития цивилизации
	В)	информационного кризиса
	Г)	информационного общества
	Д)	информационной зависимости
4.	Методы обеспечения информационной безопасности делятся (указать неправильные ответ):	
	А)	правовые
	Б)	организационно-технические
	В)	политические
	Г)	экономические
	Д)	все перечисленные выше
5.	Обеспечение защиты информации проводится конструкторами и разработчиками программного обеспечения в следующих направлениях (указать неправильный ответ):	
	А)	защита от сбоев работы оборудования
	Б)	защита от случайной потери информации
	В)	защита от преднамеренного искажения
	Г)	разработка правовой базы для борьбы с преступлениями в сфере информационных технологий
	Д)	защита от несанкционированного доступа к информации
6.	Компьютерные вирусы – это:	
	А)	вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера
	Б)	программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК
	В)	программы, являющиеся следствием ошибок в операционной системе
	Г)	пункты А) и В)
	Д)	вирусы, сходные по природе с биологическими вирусами
7.	Отличительными особенностями компьютерного вируса являются:	
	А)	значительный объем программного кода
	Б)	способность к самостоятельному запуску и многократному копированию кода
	В)	способность к созданию помех корректной работе компьютера
	Г)	легкость распознавания
	Д)	Пункты Б) и В)
8.	Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности личности, общества и государства и методы ее обеспечения?	
	А)	Уголовный кодекс РФ
	Б)	Гражданский кодекс РФ

	В)	Доктрина информационной безопасности РФ
	Г)	Постановления Правительства
	Д)	Указ Президента РФ
9.	Что не относится к объектам информационной безопасности Российской Федерации?	
	А)	природные и энергетические ресурсы
	Б)	информационные ресурсы всех видов
	В)	информационные системы различного класса и назначения, информационные технологии
	Г)	система формирования общественного сознания
	Д)	права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности
10.	Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?	
	А)	Неправомерный доступ к компьютерной информации
	Б)	Создание, использование и распространение вредоносных программ для ЭВМ
	В)	Умышленное нарушение правил эксплуатации ЭВМ и их сетей
	Г)	Все перечисленное выше
	Д)	Пункты Б) и В)
11.	Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?	
	А)	Доктрина информационной безопасности РФ
	Б)	Закон «О правовой охране программ для ЭВМ и баз данных»
	В)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Г)	Указ Президента РФ
	Д)	Закон «Об информации, информатизации и защите информации»
12.	Какой законодательный акт регулирует отношения в области защиты информационных ресурсов (личных и общественных) от искажения, порчи и уничтожения?	
	А)	Закон «Об информации, информатизации и защите информации»
	Б)	Закон «О правовой охране программ для ЭВМ и баз данных»
	В)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Г)	Пункты А) и В)
	Д)	Указ Президента РФ
13.	Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан:	
	А)	Указ Президента РФ
	Б)	Закон «Об информации, информатизации и защите информации»
	В)	Закон «О правовой охране программ для ЭВМ и баз данных»

	Г)	Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
	Д)	Доктрина национальной безопасности РФ
14.	Для написания самостоятельной работы Вы скопировали из Интернет полный текст нормативно-правового акта. Нарушили ли Вы при этом авторское право?	
	А)	да, нарушено авторское право владельца сайта
	Б)	нет, так как нормативно-правовые акты не являются объектом авторского права
	В)	нет, если есть разрешение владельца сайта
	Г)	да, нарушено авторское право автора документа
	Д)	нет, если истек срок действия авторского права
15.	Можно ли разместить на своем сайте в Интернет опубликованную в печати статью какого-нибудь автора?	
	А)	можно, с указанием имени автора и источника заимствования
	Б)	можно, с разрешения и автора статьи, и издателя
	В)	можно, но исключительно с ведома автора и с выплатой ему авторского вознаграждения
	Г)	можно, поскольку опубликованные статьи не охраняются авторским правом
	Д)	можно, с разрешения издателя, издавшего данную статью, или автора статьи
16.	Что необходимо указать при цитировании статьи, размещенной на чьем-то сайте?	
	А)	имя автора, название статьи, адрес сайта, с которого заимствована статья
	Б)	адрес сайта и имя его владельца
	В)	имя автора и название статьи
	Г)	электронный адрес сайта, с которого заимствована статья
	Д)	название статьи и название сайта
17.	Можно ли использовать статьи из разных журналов и газет на политические, экономические, религиозные или социальные темы для подготовки с их использованием учебного материала?	
	А)	нет
	Б)	да, получив согласие правообладателей
	В)	да, указав источники заимствования
	Г)	да, не спрашивая согласия правообладателей, но с обязательным указанием источника заимствования и имен авторов
	Д)	да, указав ФИО авторов и название статей
18.	Считается ли статья, обнародованная в Интернет, объектом авторского права?	
	А)	нет, если статья впервые обнародована в сети Интернет
	Б)	да, при условии, что эта же статья в течение 1 года будет опубликована в печати
	В)	да, так как любая статья является объектом авторского права как

		произведение науки или литературы
	Г)	да, если указан год первого опубликования
	Д)	да, если автор использует знак охраны авторского права
19.	В каких случаях при обмене своими компьютерными играми с другими людьми, не будут нарушаться авторские права?	
	А)	если экземпляры этих компьютерных игр были выпущены в свет и введены в гражданский оборот с согласия автора
	Б)	если обладатели обмениваемых экземпляров компьютерных игр приобрели их по договору купли-продажи/мены
	В)	если одновременно соблюдены условия, указанные в пунктах А) и Б)
	Г)	если они распространяются путем сдачи в прокат
	Д)	если автору выплачивается авторское вознаграждение
20.	В каких случаях правомерно используются фотографии из коллекции одного из Интернет-сайтов для иллюстрирования своего материала, подготавливаемого в образовательных целях?	
	А)	если тематика фото-сюжетов соответствует теме всего материала
	Б)	в любом случае, т.к. факт размещения фотографии в Интернет означает согласие автора на ее дальнейшее свободное использование
	В)	если такое использование прямо разрешено правилами Интернет-сайта
	Г)	если фотографии размещены на сайте Интернет с согласия их авторов
	Д)	Если соблюдаются условия В) и Г)

4.4. Критерии и показатели оценивания

Для текущего контроля

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.
«4»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию учителя.
«3»	устный ответ	полнота и правильность ответа, степень осознанности, понимания	ответ полный, но при этом допущена существенная ошибка, или неполный,

		изученного материала, четкость и грамотность речи.	несвязный.
«2»	устный ответ	полнота и правильность ответа, степень осознанности, понимания изученного материала, четкость и грамотность речи.	при ответе обнаружено непонимание учащимся основного содержания учебного материала или допущены существенные ошибки, которые учащийся не смог исправить при наводящих вопросах учителя.

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	практическая работа	полнота и правильность выполнения работы	работа выполнена полностью и правильно; сделаны правильные выводы.
«4»	практическая работа	полнота и правильность выполнения работы	работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.
«3»	практическая работа	полнота и правильность выполнения работы	работа выполнена правильно не менее чем на половину или допущена существенная ошибка
«2»	практическая работа	полнота и правильность выполнения работы	допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя.

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	самостоятельная работа	полнота и правильность выполнения работы	работа выполнена полностью и правильно; сделаны правильные выводы.
«4»	самостоятельная работа	полнота и правильность выполнения работы	работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.
«3»	самостоятельная работа	полнота и правильность выполнения работы	работа выполнена правильно не менее чем на половину или допущена существенная ошибка
«2»	самостоятельная	полнота и правильность	допущены две (и более) существенные ошибки в ходе

	работа	выполнения работы	работы, которые обучающийся не может исправить даже по требованию преподавателя.

Для промежуточной аттестации

Оценка	**Форма контроля**	**Критерии оценивания**	**Показатели оценивания**
«5»	тестовое задание	правильность ответа	86-100% правильных ответов на вопросы
«4»	тестовое задание	правильность ответа	71-85% правильных ответов на вопросы
«3»	тестовое задание	правильность ответа	51-70% правильных ответов на вопросы
«2»	тестовое задание	правильность ответа	0-50% правильных ответов на вопросы

5.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

5.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Организации и принципов построения информационных систем»:

, оснащенные в соответствии с п. 6.1.2.1. Примерной программы по специальности:
–Автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 8 Гб) или аналоги;
- Автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 8 Гб) или аналоги;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО: Eclipse IDE for Java EE Developers, .NETFrameworkJDK 8, Microsoft SQL Server Express Edition,
Microsoft Visio Professional, Microsoft Visual Studio,
MySQL Installer for Windows, Net Beans, SQL Server Management Studio,
Microsoft SQL Server Java Connector, Android Studio, IntelliJIDEA.

.

6.Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендованные ФУМО, для использования в образовательном процессе. При формировании библиотечного фонда образовательной организацией выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список, может быть дополнен новыми изданиями.

6.1. Основные издания

1. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И.

Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2025. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528