УТВЕРЖДЕНО:
Ученым советом ФГБОУ ВО «РГУТИС»
Протокол № 8 от « 19 » января 2026г.

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ
ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

по специальности: ***09.02.12 Техническая эксплуатация и сопровождение информационных систем***

Квалификация: ***Специалист по технической эксплуатации и сопровождению информационных систем***

год начала подготовки: 2026

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 «Основы информационной безопасности»

1.1 Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина «Основы информационной безопасности» является вариативной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

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

Осваиваемые компетенции

Код ОК, ПК	**Уметь**	**Знать**	**Владеть навыками**
ОК.01	– распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части	– актуальный профессиональный и социальный контекст, в котором приходится работать и жить	
ОК.02	– определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации	– номенклатура информационных источников, применяемых в профессиональной деятельности	-
ОК.03	– выявлять достоинства и недостатки коммерческой идеи	– возможные траектории профессионального развития и самообразования	-
ОК.04	– взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	– психологические особенности личности	
ОК.09	– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать	– правила чтения текстов профессиональной направленности	

	тексты на базовые профессиональные темы		
ПК 1.1	– Осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	– Возможности типовой ИС – Предметную область автоматизации – Инструменты и методы выявления требований к ИС	– Сбора в соответствии с трудовым заданием документации заказчика, связанной с его потребностями и запросами к типовой ИС – Анкетирования представителей заказчика в соответствии с трудовым заданием для выявления требований к типовой ИС
ПК 1.2	– Кодировать на языках программирования ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	– Основы современных операционных систем – Основы современных СУБД	– Разработки кода прототипа ИС и баз данных прототипа ИС в соответствии с трудовым заданием в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
ПК 1.3	– Кодировать на языках программирования ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	– Источники информации, необходимой для профессиональной деятельности в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	– Разработки кода ИС и баз данных ИС в соответствии с трудовым заданием в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
ПК 1.4	– Кодировать на языках программирования ИС – Тестировать результаты разработки ИС	– Языки программирования и работы с базами данных – Основы современных операционных систем	– Проведения тестирования разрабатываемого модуля ИС в соответствии с трудовым заданием в рамках технической поддержки процессов

			создания (модификации) и сопровождения ИС
ПК 1.5	– Тестировать результаты разработки ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	– Основы управления изменениями в проектах в области информационных технологий	– Воспроизведения зафиксированных в системе учета дефектов и несоответствий в коде ИС и документации к ИС согласно трудовому заданию в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
ПК 1.6	– Устанавливать программное обеспечение, необходимое для функционирования ИС – Деинсталлировать программное обеспечение, необходимое для функционирования ИС	– Основы системного администрирования – Основы администрирования баз данных – Коммуникационное оборудование	– Проверки соответствия рабочих мест ИС требованиям ИС к оборудованию и программному обеспечению в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
ПК 1.7	– Идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – Осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	– Основы ИБ организации – Модель угроз информационной безопасности ИС организации заказчика – Процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика	– Распознавания инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС – Передачи информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
ПК 2.1	– Работать в современном текстовом	– Основные возможности	– Создания шаблона документа

	процессоре – Создавать, настраивать, применять стили в документе с помощью текстового процессора – Создавать графические схемы, получать снимки экрана, включать рисунки в технический документ и оформлять их	современных текстовых процессоров – Основные стандарты оформления текстовых документов – Основные способы работы с векторной и растровой графикой, способы включения рисунков в документ, правила оформления рисунков	для заданного текстового процессора – Применения к тексту документа средств оформления – Создания в документе информационно-поискового аппарата
ПК 2.2	– Находить в информационно-телекоммуникационной сети "Интернет" источники информации по заданной теме – Пользоваться ресурсами научно-технических библиотек и архивов	– Научно-технический стиль изложения и его особенности – Основные разновидности научно-технических документов – Основные стандарты оформления научно-технических отчетов	– Разработки структуры документа и ее согласование с экспертами – Подбора дополнительных источников информации
ПК 2.3	– Устанавливать и настраивать программные средства, предназначенные для работы со структурированным контентом	– Языки разметки, основные типы языков разметки (теговые, легковесные) и их особенности в объеме, необходимом для выполнения трудовой функции	– Выбора, установки, настройки программных средств для ввода и структурирования контента с использованием заданного языка разметки
ПК 2.4	– Работать с системой управления задачами и/или системой контроля версий – Логически группировать изменения на новые, обновленные и исправленные ошибки	– Системы управления задачами и системы контроля версий: поиск и выделение нужной информации	– Получения из задачи в системе управления задачами или из системы управления версиями последних изменений в программном продукте
ПК 2.5	– Работать с текстом как с объектом исследования	– Основные подходы к оценке качества технической	– Сбора исходных данных для оценки качества технической

	– Использовать электронные таблицы для статистических вычислений – Составлять аналитические отчеты на основе данных статистики	документации – Основные метрики качества технической документации	документации – Расчета значений заданных метрик качества технической документации Составления отчета об оценке качества технической документации
ПК 2.6	– Оценивать правовые и этические аспекты технологий и их применения. – Четко и понятно объяснять правовые требования и последствия их несоблюдения как техническим, так и нетехническим сотрудникам.	– Основы гражданского, административного и уголовного права, касающихся информационных технологий.	– Умения анализировать и интерпретировать законодательные и нормативные документы, касающиеся информационных технологий.

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	64
в т.ч. в форме практической подготовки (если предусмотрено)	-
в т. ч.:	
теоретическое обучение	18
практические и лабораторные занятия *(если предусмотрено)*	30
Самостоятельная работа	2
Консультации	2
Промежуточная аттестация (Экзамен в 4 семестре)	12

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий, *курсовой проект (работа)*	Обьем часов	Коды компетенций, формированию которых способствует элемент программы
Тема 1. Введение в информационную безопасность	**Содержание**		
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе самостоятельная работа обучающихся Систематическая проработка конспектов занятий, учебной и специальной технической литературы по темам: 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.	**1**	
Тема 2. Управление безопасностью информации	**Содержание**		
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
Тема 3. Криптография	**Содержание**		
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических занятий		

	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	6	
Тема 4. Защита сетевой инфраструктуры	**Содержание**		
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	1	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических и лабораторных занятий		
	Организация защиты от атак	4	
	Организация работы VPN и межсетевого экрана	4	
Тема 5. Безопасность приложений	**Содержание**		
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических и лабораторных занятий		
	Тестирование на проникновение и анализ уязвимостей.	4	
Тема 6. Защита данных	**Содержание**		
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических и лабораторных занятий		
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным	6	
Тема 7. Безопасность облачных технологий	**Содержание**		
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	1	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических и лабораторных занятий		
	Изучение модели облачных услуг и их безопасности	2	

Тема 8. Инциденты безопасности	**Содержание**		
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических и лабораторных занятий		
	Работа с инцидентами.	2	
Тема 9. Социальная инженерия и человеческий фактор	**Содержание**		
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе практических и лабораторных занятий		
	Разработка политики информационной безопасности	2	
Тема 10. Будущее информационной безопасности	**Содержание**		
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	2	**ОК 01- ОК 04, ОК 09, ПК 1.1 - ПК 2.6**
	В том числе самостоятельная работа обучающихся Систематическая проработка конспектов занятий, учебной и специальной технической литературы по темам: 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.	**1**	
Промежуточная аттестация		***12***	

Консультации	***2***	
Всего 64 часа		

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 3. Криптография
№1 Работа с симметричными и асимметричными алгоритмами.
№2 Хэширование и создание цифровой подписи сообщения.

Тема 4. Защита сетевой инфраструктуры
№3 Организация защиты от атак
№4 Организация работы VPN и межсетевого экрана

Тема 5. Безопасность приложений
№5 Тестирование на проникновение и анализ уязвимостей

Тема 6. Защита данных
№6 Выполнение резервного копирования и восстановления данных.
№7 Управление доступом к данным

Тема 7. Безопасность облачных технологий
№8 Изучение модели облачных услуг и их безопасности

Тема 8. Инциденты безопасности
№9 Работа с инцидентами.

Тема 9. Социальная инженерия и человеческий фактор
№10 Разработка политики информационной безопасности

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
4	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	Эксплуатация подсистем управления информацион-ной безопасностью различных объектов	*Для текущего контроля:* оценка результатов практических занятий; *Для промежуточной аттестации:*

безопасностью различных объектов информатизации;	информатизации	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 эффективного использования различных типов технологических систем и способов обработки и хранения традиционных	- соответствие способов достижения цели, способам определенным руководителем и документами;	*Для текущего контроля:* устный опрос. *Для промежуточной аттестации:* экзамен

и электронных конфиденциальных документов;		

Формируемые компетенции:

Код формируемой компетенции	Наименование компетенции	Формы и методы контроля и оценки результатов обучения
ОК 01	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 02	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 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 1.1	Осуществлять сбор данных для выявления требований к	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос.

	типовой информационной системе в соответствии с техническим заданием.	*Для промежуточной аттестации:* экзамен
ПК 1.2	Разрабатывать прототипы информационных систем в соответствии с техническим заданием.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 1.3	Осуществлять написание программного кода информационных систем в соответствии с техническим заданием.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 1.4	Выполнять тестирование информационных систем (верификацию) в соответствии с техническим заданием.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 1.5	Исправлять дефекты и несоответствия в коде информационных систем и документации к информационным системам.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 1.6	Развертывать рабочие места информационных систем у заказчика.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 1.7	Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 2.1	Оформлять техническую документацию на продукцию в сфере информационно-коммуникационных	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:*

	технологий.	экзамен
ПК 2.2	Разрабатывать техническую и эксплуатационную документацию программных решений.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 2.3	Осуществлять разметку контента технической документации.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 2.4	Осуществлять поддержку технической документации в актуальном состоянии.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 2.5	Проводить оценку качества технической документации с использованием заданной системы показателей.	*Для текущего контроля:* оценка работы на практических занятиях, устный опрос. *Для промежуточной аттестации:* экзамен
ПК 2.6	Соблюдать нормативные правовые акты в сфере информационных технологий.	*Для текущего контроля:* оценка работы на практических занятиях, 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.**

Перечень теоретических вопросов:

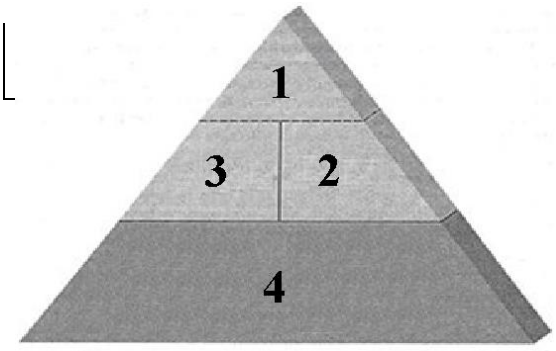
1 Главная цель мер, предпринимаемых на административном уровне:

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 изученного материала, четкость и грамотность речи.	ответ полный, но при этом допущена существенная ошибка, или неполный, 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.

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 «Основ информационной безопасности»:

№	**Наименование**	**Тип**	**Основное/ специализированное**	**Краткая (рамочная) техническая характеристика**
1	Посадочные места по количеству обучающихся (столы, стулья)	Мебель	Основное	На усмотрение ОО
2	Рабочее место преподавателя	Мебель	Основное	На усмотрение ОО
3	Шкаф или полки для хранения учебной и методической литературы	Мебель	Основное	На усмотрение ОО
4	Доска маркерная	Мебель	Основное	На усмотрение ОО
5	ПК преподавателя (системный блок, монитор, клавиатура, мышь)	ТС	Основное	ЦПУ: - Intel(R) Core(TM) i3-10100 - количество физических ядер - 4 - количество потоков - 8 Сетевой адаптер: - технология Ethernet - 10/100/1000 mbps ОЗУ: - 8 ГБ Графический адаптер: - NVIDIA GeForce GT730

№	Наименование	Тип	Основное/ специализированное	Краткая (рамочная) техническая характеристика
				ПЗУ:- SSD 256 ГБ
6	ПК (системный блок, монитор, клавиатура, мышь) по количеству обучающихся	ТС	Основное	ЦПУ: - Intel(R) Core(TM) i3-10100 - количество физических ядер - 4 - количество потоков - 8 Сетевой адаптер: - технология Ethernet - 10/100/1000 mbps ОЗУ: - 8 ГБ Графический адаптер: - NVIDIA GeForce GT730 ПЗУ:- SSD 256 ГБ
7	Мультимедийный проектор	ТС	Основное	На усмотрение ОО
8	Аудио- и видеооборудование	ТС	Основное	На усмотрение ОО
9	Комплект учебно-методических материалов	УМК	Основное	На усмотрение ОО

№ п/п	Наименование лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
1	Операционная система (РЕД ОС 8.0 или аналог)
2	Клиент для работы с API (Postman или аналог)
3	Программное обеспечение для записи экрана (OBS Studio или аналог)
4	Эмулятор выполняемой среды (Genymotion, VirtualBox, VMWare Workstation или аналог)
5	Набор средств разработки (Node.js или аналог)
6	ПО веб-браузер (Яндекс Браузер, Chromium, Google Chrome или аналоги)
7	ПО Системы контроля версий (Git, GitKraken или аналоги)
8	Текстовый редактор (Sublime Text, Visual Studio Code или аналоги)

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