МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)
Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) **Документ подписан простой электронной подписью**

Сертификат: 00fd759708ffd39703
Владелец: Бачевский Сергей Викторович
Действителен с 15.03.2021 по 14.03.2026

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ О.В. Колбанева
_____ 2021 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование учебной дисциплины)

программа подготовки специалистов среднего звена

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2021

Комплект контрольно-оценочных средств составлен в соответствии с ППССЗ по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и рабочей программой по учебной дисциплине «Основы информационной безопасности»

Составитель
Преподаватель _____ Н.В. Кривоносова
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 5 (информатики и программирования в компьютерных системах)
07 апреля 2021 г., протокол № 8

Председатель предметной (цикловой) комиссии: _____ Н.В. Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций
21 апреля 2021 г., протокол № 6

Оглавление

ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

Результатом освоения дисциплины Основы информационной безопасности является освоение обучающимся материала в объёме предусмотренном ФГОС СПО по специальности 10.02.04. Обеспечение информационной безопасности телекоммуникационных систем и рабочей программой по дисциплине, а также формирование общих и профессиональных компетенций в процессе освоения ППССЗ в целом.

Форма промежуточной аттестации –дифференцированный зачет.

1. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Показатели оценки результата

В результате контроля и оценки по дисциплине осуществляется комплексная проверка следующих общих и профессиональных компетенций:

Таблица 1

Код компетенции	Содержание компетенции	Показатели оценки результата (знания, умения)
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие	Умения: – определять актуальность нормативно-правовой документации в профессиональной деятельности; – выстраивать траектории профессионального и личностного развития Знания: – содержание актуальной нормативно-правовой документации; – современная научная и профессиональная терминология; – возможные траектории профессионального развития и самообразования
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Умения: – описывать значимость своей профессии; – презентовать структуру профессиональной деятельности по профессии (специальности). Знания: – сущность гражданско-патриотической позиции; – общечеловеческие ценности; – правила поведения в ходе выполнения профессиональной деятельности.
ОК 09	Использовать информационные технологии в профессиональной деятельности	Умения: – применять средства информационных технологий для решения профессиональных задач; – использовать современное программное обеспечение. Знания: – современные средства и устройства информатизации; – порядок их применения и программное обеспечение в профессиональной

		деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранных языках.	Умения: – понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; – участвовать в диалогах на знакомые общие и профессиональные темы; – строить простые высказывания о себе и о своей профессиональной деятельности; – кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы. Знания: – правила построения простых и сложных предложений на профессиональные темы; – основные общеупотребительные глаголы (бытовая и профессиональная лексика); – лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; – особенности произношения; – правила чтения текстов профессиональной направленности.

Таблица 2

Профессиональные компетенции	**Наименование компетенции**
ПК 2.1	Проводить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей

1.2. Требования к знаниям и умениям

Таблица 3

Уметь:	
У-1	классифицировать защищаемую информацию по видам тайны и степеням секретности
У-2	классифицировать основные угрозы безопасности информации.
Знать:	
З-1	сущность и понятие информационной безопасности, характеристику ее составляющих;
З-2	место информационной безопасности в системе национальной безопасности страны;
З-3	виды, источники и носители защищаемой информации;
З-4	источники угроз безопасности информации и меры по их предотвращению;
З-5	факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

З-6	жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
З-7	современные средства и способы обеспечения информационной безопасности;
З-8	основные методики анализа угроз и рисков информационной безопасности;

1.3. Матрица компетенций по дисциплине

Таблица 4

Элемент КОС	Проверяемые общие и профессиональные компетенции (знания, умения)						
	ОК 03	ОК 06	ОК 09	ОК 10	ПК 2.1	У - 1	У - 2
ПЗ №1	+	+	+	+	+	+	+
ПЗ №2	+	+	+	+	+	+	+
ПЗ №3	+	+	+	+	+	+	+
ПЗ №4	+	+	+	+	+	+	+
ПЗ №5	+	+	+	+	+	+	+
ПЗ №6	+	+	+	+	+	+	+
ПЗ №7	+	+	+	+	+	+	+
ПЗ №8	+	+	+	+	+	+	+
ПЗ №9	+	+	+	+	+	+	+

Оценочные материалы для практических занятий - см. Методические рекомендации к выполнению практических занятий дисциплины ОП.04 Обеспечение информационной безопасности.

2. ОЦЕНКА ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Формы и методы оценивания

Основной целью оценки теоретического курса дисциплины «Основы информационной безопасности» является оценка умений и знаний.

Оценка осуществляется с использованием следующих форм и методов контроля согласно п.2.6 и п.2.10 Положения о текущем контроле успеваемости обучающихся Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля:

- *текущий контроль*:
  - устный опрос на лекциях, практические и семинарские занятия;
  - практические задания;
  - самостоятельные работы;
  - контрольные работы;
  - защита лабораторных работ;
  - контроль самостоятельной работы (в письменной или устной форме);
  - тестирование (письменное или компьютерное);
- *рубежный контроль*:
  - тестирование (письменное или компьютерное);
  - контрольные работы;
  - прием индивидуальных домашних заданий, рефератов, отчетов по лабораторным работам.

Текущий контроль обеспечивают типовые задания:

Таблица 5

Элемент учебной дисциплины	Результаты обучения	Формы текущего контроля
Раздел 1. Теоретические основы информационной безопасности		
Тема 1.1. Основные понятия и задачи информационной безопасности	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	устный опрос, тестирование
Тема 1. 2. Основы защиты информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	устный опрос, защита отчета по практическому занятию
Тема 1. 3. Угрозы безопасности защищаемой информации.	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	устный опрос, защита отчета по практическому занятию
Раздел 2. Методология защиты информации		
Тема 2.1. Методологические подходы к защите информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	устный опрос, тестирование
Тема 2.2 Нормативно правовое регулирование защиты информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	устный опрос, защита отчета по практическому занятию
Тема 2.3. Защита информации в автоматизированных (информационных) системах	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1,	устный опрос, защита отчета по практическому занятию

2.2. Типовые задания для оценки освоения дисциплины

2.2.1. Тестовые вопросы по Разделу 1. Теоретические основы информационной безопасности

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Слово "криптография" произошло от	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
2	Для чего используется система Kerberos?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
3	Наука об обеспечении секретности и или аутентичности (подлинности) передаваемых сообщений	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
4	Замену символов с открытого текста, соответствующими символами алфавита криптотекста называют	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90

5	Процесс применения шифра защищаемой информации называют	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
6	Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
7	Как называется процесс наложения по определенному закону гамма-шифра на открытые данные	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
8	Какой спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
9	Как называется криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
10	Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
11	Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
12	Совокупность действий (инструкций, команд, вычислений), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
13	Какова разрядность ключа алгоритма шифрования ГОСТ 28147 – 89 (первого российского стандарта шифрования)	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
14	Как называется состояние информационной среды, в котором обеспечены конфиденциальность, целостность и доступность информации?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
15	Перехват, который осуществляется путем использования оптической техники называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
16	Как называется информация в электронной форме, которая присоединена к другой информации в электронной форме, используемая для определения лица, подписавшего информацию?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
17	По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
18	Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи - это	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90

Закрытые вопросы

№	Вопрос	ОК/ПК	Время, сек
1	В чем заключается основная причина потерь информации, связанной с ПК? А. С глобальным хищением информации Б. С появлением интернета	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

	В. С недостаточной образованностью в области безопасности		
2	Технические средства защиты информации – это А. средства, которые реализуются в виде автономных устройств и систем Б. устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу В. программы, предназначенные для выполнения функций, связанных с защитой информации Г. средства, которые реализуются в виде электрических, электромеханических и электронных устройств	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
3	К аспектам ИБ относятся А. Дискретность Б. Целостность В. Конфиденциальность Г. Актуальность Д. Доступность	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
4	Что такое криптология? А. Защищенная информация Б. Область доступной информации В. Тайная область связи	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
5	Что такое несанкционированный доступ (НСД)? А. Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа Б. Создание резервных копий в организации В. Правила и положения, выработанные в организации для обхода парольной защиты Г. Вход в систему без согласования с руководителем организации Д. Удаление не нужной информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
6	Что такое целостность информации? А. Свойство информации, заключающееся в возможности ее изменения любым субъектом Б. Свойство информации, заключающееся в возможности изменения только единственным пользователем В. Свойство информации, заключающееся в ее существовании в виде единого набора файлов Г. Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
7	Кто является знаковой фигурой в сфере информационной безопасности А. Митник Б. Шеннон В. Паскаль Г. Беббидж	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
8	Под ИБ понимают А. защиту от несанкционированного доступа Б. защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера В. защиту информации от компьютерных вирусов	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

9	Что такое аутентификация? А. Проверка количества переданной и принятой информации Б. Нахождение файлов, которые изменены в информационной системе несанкционированно В. Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа) Г. Определение файлов, из которых удалена служебная информация Д. Определение файлов, из которых удалена служебная информация	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
10	Верификация – это А. проверка принадлежности субъекту доступа предъявленного им идентификатора. Б. проверка целостности и подлинности инф, программы, документа В. присвоение имени субъекту или объекту	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
11	Кодирование информации – это А. представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д. Б. метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
12	Утечка информации – это А. несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу Б. ознакомление постороннего лица с содержанием секретной информации В. потеря, хищение, разрушение или неполучение переданных данных	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
13	Линейное шифрование – это А. несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу Б. криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому В. криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
14	Угроза – это А. возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов Б. событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
15	Основными рисками информационной безопасности являются А. искажение, уменьшение объема, перекодировка информации Б. техническое вмешательство, выведение из строя оборудования сети В. потеря, искажение, утечка информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
16	К основным функциям системы безопасности можно отнести А. установление регламента, аудит системы, выявление рисков Б. установку новых офисных приложений, смену хостинг-компании В. внедрение аутентификации, проверка контактных данных пользователей	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

17	Принципом политики информационной безопасности является принцип А. усиления защищенности самого незащищенного звена сети (системы) Б. перехода в безопасное состояние работы сети, системы В. полного доступа пользователей ко всем ресурсам сети, системы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
18	ЭЦП – это А. электронно-цифровой преобразователь Б. электронно-цифровая подпись В. электронно-цифровой процессор	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
19	Наиболее распространены угрозы информационной безопасности корпоративной системы А. Покупка нелицензионного ПО Б. Ошибки эксплуатации и неумышленного изменения режима работы системы В. Сознательного внедрения сетевых вирусов	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
20	Утечкой информации в системе называется ситуация, характеризуемая А. потерей данных в системе Б. изменением формы информации В. изменением содержания информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
21	Угроза информационной системе (компьютерной сети) – это А. вероятное событие Б. детерминированное (всегда определенное) событие В. событие, происходящее периодически	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
22	Угроза – это А. потенциальная возможность определенным образом нарушить информационную безопасность Б. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных В. процесс определения отвечает на текущее состояние разработки требованиям данного этапа	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
23	Атака – это А. попытка реализации угрозы Б. потенциальная возможность определенным образом нарушить информационную безопасность В. программы, предназначенные для поиска необходимых программ.	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
24	Источник угрозы – это А. потенциальный злоумышленник Б. злоумышленник В. нет правильного ответа	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

25	Криптографические средства – это А. специальные программы и системы защиты информации в информационных системах различного назначения Б. средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования В. механизм, позволяющий получить новый класс на основе существующего	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

2.2.2. Тестовые вопросы по Разделу 2. Методология защиты информации

Открытые вопросы

№	Вопрос	ОК/ПК	Время, сек
1	Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
2	Надежность СЗИ определяется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
3	Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
4	Недостатком дискретных моделей политики безопасности является	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
5	Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
6	Обеспечением скрытности информации в информационных массивах занимается наука	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
7	По документам ГТК количество классов защищенности СВТ от НСД к информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
8	По документам ГТК самый низкий класс защищенности СВТ от НСД к информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
9	Совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
10	При избирательной политике безопасности в матрице доступа объекту системы соответствует	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
11	Где представлены совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90

12	При односторонней аутентификации осуществляется аутентификация …	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
13	Кто в компании является основным ответственным за определение уровня классификации информации?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
14	Какая категория людей является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
15	Кто в компании в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90

Закрытые вопросы

№	Вопрос	ОК/ПК	Время, сек
1	В чем состоит задача криптографа? А. Взломать систему защиты Б. Обеспечить конфиденциальность и аутентификацию передаваемых сообщений	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
2	Под изоляцией и разделением (требование к обеспечению ИБ) понимают А. разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов) Б. разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
3	К аспектам ИБ относятся А. Дискретность Б. Целостность В. Конфиденциальность Г. Актуальность Д. Доступность	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
4	Прочность защиты в АС – это А. вероятность не преодоления защиты нарушителем за установленный промежуток времени Б. способность системы защиты информации обеспечить достаточный уровень своей безопасности В. группа показателей защиты, соответствующая определенному классу защиты	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
5	Уровень секретности – это А. ответственность за модификацию и НСД информации Б. административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
6	К правовым методам, обеспечивающим информационную безопасность, относятся	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

	А. разработка аппаратных средств обеспечения правовых данных Б. разработка и установка во всех компьютерных правовых сетях журналов учета действий В. разработка и конкретизация правовых нормативных актов обеспечения безопасности		
7	Основными источниками угроз информационной безопасности являются все указанное в списке А. Хищение жестких дисков, подключение к сети, инсайдерство Б. Перехват данных, хищение данных, изменение архитектуры системы В. Хищение данных, подкуп системных администраторов, нарушение регламента работы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
8	Основные объекты информационной безопасности А. Компьютерные сети, базы данных Б. Информационные системы, психологическое состояние пользователей В. Бизнес-ориентированные, коммерческие системы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
9	К основным принципам обеспечения информационной безопасности относится А. экономическая эффективность системы безопасности Б. многоплатформенная реализации системы В. усиление защищенности всех звеньев системы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
10	Основные субъекты информационной безопасности А. Руководители, менеджеры, администраторы компаний Б. Органы права, государства, бизнеса В. Сетевые базы данных, фаерволлы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
11	Принципом информационной безопасности является принцип недопущения А. неоправданных ограничений при работе в сети (системе) Б. рисков безопасности сети, системы В. презумпции секретности	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
12	Принципом политики информационной безопасности является принцип А. невозможности миновать защитные средства сети (системы) Б. усиления основного звена сети, системы В. полного блокирования доступа при риск-ситуациях	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
13	Принципом политики информационной безопасности является принцип А. разделения доступа (обязанностей, привилегий) клиентам сети (системы) Б. одноуровневой защиты сети, системы В. совместимых, однотипных программно-технических средств сети, системы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
14	Когда получен спам по e-mail с приложенным файлом, следует А. прочитать приложение, если оно не содержит ничего ценного – удалить	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

	Б. сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама В. удалить письмо с приложением, не раскрывая (не читая) его		
15	Окончательно, ответственность за защищенность данных в компьютерной сети несет А. владелец сети Б. администратор сети В. пользователь сети	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
16	Политика безопасности в системе (сети) – это комплекс А. руководств, требований обеспечения необходимого уровня безопасности Б. инструкций, алгоритмов поведения пользователя в сети В. нормы информационного права, соблюдаемые в сети	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
17	Суть компрометации информации А. Внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации Б. Несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений В. Внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
18	Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, А. с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды Б. с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации В. способна противостоять только информационным угрозам, как внешним, так и внутренним Г. способна противостоять только внешним информационным угрозам	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
19	Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ) А. МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения Б. МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты В. МЭ работают только на сетевом уровне, а СОВ – еще и на физическом	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

2.2.3. Тестовые вопросы итогового тестирования по дисциплине ОП.04 «Основы информационной безопасности»

Открытые вопросы

№	Вопрос	ОК/ПК	Время, сек
1	Как называется информация в электронной форме, которая присоединена к другой информации в электронной форме, используемая для определения лица, подписавшего информацию?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
2	Какие из средств защиты информации направлены на защиту оборудования?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
3	Как называется состояние информационной среды, в котором обеспечены конфиденциальность, целостность и доступность информации?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
4	Сколько статей в разделе «Преступления в сфере компьютерной информации» уголовного кодекса РФ?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	120
5	Правовые отношения между кем регулирует Федеральный закон о персональных данных?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	180
6	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
7	К какому типу мер по защите информации относится установка уплотнителей в дверном проеме защищаемого помещения?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
8	Какой орган государственной власти является правопреемником Гостехкомиссии России?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
9	По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
10	Какие меры защиты информации предусматривают использование конструктивных решений и технологических особенностей обработки информации ограниченного доступа на объектах информатизации?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
11	При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
12	Можно ли в качестве активной технической меры выбрать установку сертифицированной антивирусной программы?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
13	Какие стороны участвуют в процессе лицензирования?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
14	Оценка возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями проводится при …	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90

15	Когда произошло становление отечественного законодательства по информатизации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
16	Какой документ определяет на международном уровне пределы вмешательства в частную жизнь со стороны государства и других субъектов?	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
17	Перехват информации, который предполагает использование оборудования для несанкционированного съема информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
18	Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
19	Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
20	Перехват, который осуществляется путем использования оптической техники называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
21	Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
22	Программный модуль, кото-рый имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему, является клавиатурным шпионом типа	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
23	С помощью закрытого ключа информация	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
24	С точки зрения ГТК основной задачей средств безопасности является обеспечение	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
25	Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
26	Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
27	Наукой, изучающей математические методы защиты информации путем ее преобразования, является	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	120
28	Главным параметром криптосистемы является показатель	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	120
29	Установление санкционированным получателем (приемником) того факта, что полученное сообщение послано санкционированным отправителем (передатчиком) называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90
30	Совокупность действий (инструкций, команд, вычислений), выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата называется	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	90

Закрытые вопросы

№	Вопрос	ОК/ПК	Время, сек
1	К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками…» А. Информация без ограничения права доступа Б. Информация с ограниченным доступом В. Информация, распространение которой наносит вред интересам общества Г. Объект интеллектуальной собственности Д. Иная общедоступная информация	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
2	Под какие системы распространение вирусов происходит наиболее динамично: А. Android Б. Windows В. Mac OS Г. Linux	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
3	Под угрозой удаленного администрирования в компьютерной сети понимается угроза А. несанкционированного управления удаленным компьютером Б. внедрения агрессивного программного кода в рамках активных объектов Web-страниц В. перехвата или подмены данных на путях транспортировки Г. вмешательства в личную жизнь Д. поставки неприемлемого содержания	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
4	К формам защиты информации не относится А. Аналитическая Б. Правовая В. Организационно-техническая Г. Страховая	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
5	Какие существуют основные уровни обеспечения защиты информации? А. Законодательный Б. Административный В. Программно-технический Г. Физический Д. Вероятностный Е. Процедурный Ж. Распределительный	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
6	К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право…» А. Информация без ограничения права доступа Б. Информация с ограниченным доступом В. Информация, распространение которой наносит вред интересам общества Г. Объект интеллектуальной собственности Д. Иная общедоступная информация	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

7	Информация, составляющая государственную тайну не может иметь гриф А. «Для служебного пользования» Б. «Секретно» В. «Совершенно секретно» Г. «Особой важности»	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
8	Какие трудности возникают в информационных системах при конфиденциальности? А. Сведения о технических каналах утечки информации являются закрытыми Б. На пути пользовательской криптографии стоят многочисленные технические проблемы В. Все ответы правильные	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
9	Суть компрометации информации А. Внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации Б. Несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений В. Внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
10	К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия…» А. Информация без ограничения права доступа Б. Информация с ограниченным доступом В. Информация, распространение которой наносит вред интересам общества Г. Объект интеллектуальной собственности Д. Иная общедоступная информация	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
11	Основными источниками угроз информационной безопасности являются все указанное в списке А. Хищение жестких дисков, подключение к сети, инсайдерство Б. Перехват данных, хищение данных, изменение архитектуры системы В. Хищение данных, подкуп системных администраторов, нарушение регламента работы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
12	Виды информационной безопасности А. Персональная, корпоративная, государственная Б. Клиентская, серверная, сетевая В. Локальная, глобальная, смешанная	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
13	Наиболее эффективное средство для защиты от сетевых атак А. Использование сетевых экранов или «firewall» Б. Использование антивирусных программ	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

	В. Посещение только «надёжных» Интернет-узлов Г. Использование только сертифицированных программ-браузеров при доступе к сети Интернет		
14	Атака – это А. попытка реализации угрозы Б. потенциальная возможность определенным образом нарушить информационную безопасность В. программы, предназначенные для поиска необходимых программ.	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
15	Источник угрозы – это А. потенциальный злоумышленник Б. злоумышленник В. нет правильного ответа	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
16	Программные средства – это А. модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними Б. структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла В. специальные программы и системы защиты информации в информационных системах различного назначения	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
17	К вирусам, изменяющим среду обитания относятся А. черви Б. студенческие В. полиморфные Г. спутники	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
18	Наиболее распространенные средства воздействия на сеть офиса А. Слабый трафик, информационный обман, вирусы в интернет Б. Вирусы в сети, логические мины (закладки), информационный перехват В. Компьютерные сбои, изменение администрирования, топологии	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
19	Утечкой информации в системе называется ситуация, характеризуемая А. потерей данных в системе Б. изменением формы информации В. изменением содержания информации	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
20	Какие вирусы активизируются в самом начале работы с операционной системой? А. Загрузочные вирусы Б. Черви В. Трояны	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
21	Под ИБ понимают А. защиту от несанкционированного доступа Б. защиту информации от случайных и преднамеренных воздействий естественного и искусственного характера В. защиту информации от компьютерных вирусов	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

22	Что такое аутентификация? А. Проверка количества переданной и принятой информации Б. Нахождение файлов, которые изменены в информационной системе несанкционированно В. Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа) Г. Определение файлов, из которых удалена служебная информация Д. Определение файлов, из которых удалена служебная информация	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
23	Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов А. Компаньон-вирусы Б. Черви В. Паразитические Г. Студенческие Д. Призраки Е. Стелс-вирусы Ж. Макровирусы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
24	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? А. Хакеры Б. Сотрудники В. Контрагенты	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
25	Основные субъекты информационной безопасности А. Руководители, менеджеры, администраторы компаний Б. Органы права, государства, бизнеса В. Сетевые базы данных, фаерволлы	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
26	Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это А. идентификатор пользователя Б. пароль пользователя В. учетная запись пользователя Г. парольная система	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
27	Технические средства защиты информации – это А. средства, которые реализуются в виде автономных устройств и систем Б. устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу В. программы, предназначенные для выполнения функций, связанных с защитой информации Г. средства, которые реализуются в виде электрических, электромеханических и электронных устройств	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

28	Таргетированная атака – это А. атака на сетевое оборудование Б. атака на конкретный компьютер пользователя В. атака на компьютерную систему крупного предприятия	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
29	Главным параметром криптосистемы является показатель А. безошибочности шифрования Б. скорости шифрования В. криптостойкости Г. надежности функционирования	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45
30	К видам системы обнаружения атак относятся А. системы, обнаружения атаки на ОС Б. системы, обнаружения атаки на конкретные приложения В. системы, обнаружения атаки на удаленных БД Г. все варианты верны	ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.1	45

2.3. Критерии оценок по типам (видам) заданий

№	Тип (вид) задания	Критерии оценки
1	Устные ответы, письменные развернутые ответы	**Оценка «5»** ставится в том случае, если обучающийся правильно понимает сущность вопроса, дает точное определение и истолкование основных понятий; правильно анализирует условие задачи (вопроса), ответ логичен, умеет выстроить алгоритм поиска ответа самостоятельно; строит ответ по собственному плану, сопровождает ответ новыми примерами, умеет применить знания в новой ситуации; может установить связь между изучаемым и ранее изученным материалом из курса дисциплины, а также с материалом, усвоенным при изучении других дисциплин/модулей. **Оценка «4»** ставится, если ответ обучающегося удовлетворяетосновным требованиям к ответу на оценку 5, но дан без использования собственного плана, новых примеров, без применения знаний в новой ситуации, без использования связей с ранее изученным материалом и материалом, усвоенным при изучении других дисциплин/модулей; обучающийся допустил одну ошибку или не более двух недочетов и может их исправить самостоятельно или с небольшой помощью преподавателя. **Оценка «3»** ставится, если обучающийся правильно понимает сущность вопроса, но в ответе имеются отдельные пробелы в усвоении вопросов курса дисциплины, не препятствующие дальнейшему усвоению программного материала; умеет применять полученные знания при решении простых задач (заданий, вопросов) по готовому алгоритму; допустил не более одной грубой ошибкии двух недочетов, не более одной грубой и одной негрубой ошибки, не более двух-трех негрубых ошибок, одной негрубой ошибки и трех недочетов; допустил четыре-пять недочетов. **Оценка «2»** ставится, если обучающийся не овладел основными знаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для оценки.

2	Тесты	**«5»** - 100 – 85% правильных ответов **«4»** - 84 - 70% правильных ответов **«3»** - 69 – 52% правильных ответов **«2»** - 51% и менее правильных ответов
3	Доклады, рефераты, эссе, творческие работы	**Оценка «5»** ставится, если выполнены все требования к написанию и защите работы: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. **Оценка «4»** основные требования к работе и её защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы. **Оценка «3»** имеются существенные отступления от требований к работе. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. **Оценка «2»** тема не раскрыта, обнаруживается существенное непонимание проблемы.
4	Практические задания Лабораторные работы	**Оценка «5»** выставляется, если обучающийся активно работает в течение всего практического занятия, дает полные ответы на вопросы преподавателя в соответствии с планом практического занятия и показывает при этом глубокое овладение лекционным материалом, способен выразить собственное отношение по данной проблеме, проявляет умение самостоятельно и аргументированно излагать материал, анализировать явления и факты со ссылками на соответствующие источники, делать самостоятельные обобщения и выводы, заключения, рекомендации, правильно выполняет все этапы практического задания. **Оценка «4»** выставляется при условии соблюдения следующих требований: обучающийся активно работает в течение практического занятия, вопросы освещены полно, изложения материала логическое, обоснованное фактами, со ссылками на соответствующие источники, освещение вопросов завершено выводами, обучающийся обнаружил умение анализировать факты и события, а также выполнять учебные задания. Но в ответах допущены неточности, некоторые незначительные ошибки, имеет место недостаточная аргументированность при изложении материала, недостаточно четко сделаны обобщение и выводы. **Оценка «3»** выставляется в том случае, когда обучающийся в целом овладел сути вопросов по данной теме, обнаруживает знание лекционного материала и учебной

		литературы, пытается анализировать факты и события, делать выводы и решать задачи. Но на занятии ведет себя пассивно, отвечает только по вызову преподавателя, дает неполные ответы на вопросы, допускает грубые ошибки при освещении теоретического материала, не может обобщить и сделать четкие логические выводы. **Оценка «2»** выставляется в случае, когда обучающийся обнаружил несостоятельность осветить вопросы или вопросы освещены неправильно, бессистемно, с грубыми ошибками, отсутствуют понимания основной сути вопросов, выводы, обобщения, обнаружено неумение решать учебные задачи.

2.4. Фонд оценочных средств для промежуточной аттестации по учебнойдисциплине ОП.04 «Основы информационной безопасности»

ПАСПОРТ

Назначение:

Контрольно-оценочные материалы предназначены для контроля и оценки результатов освоения учебной дисциплины ОП.04 Основы информационной безопасности по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, базового уровня подготовки.

Вопросы к дифференцированному зачету по дисциплине ОП.04 «Основы информационной безопасности»

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации».
5. Понятие «риска информационной безопасности».
6. Примеры преступлений в сфере информации и информационных технологий.
7. Сущность функционирования системы защиты информации.
8. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
9. Целостность, доступность и конфиденциальность информации.
10. Классификация информации по видам тайны и степеням конфиденциальности.
11. Понятия государственной тайны и конфиденциальной информации.
12. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
13. Цели и задачи защиты информации. Основные понятия в области защиты информации.
14. Элементы процесса менеджмента ИБ.
15. Модель интеграции информационной безопасности в основную деятельность организации.
16. Понятие Политики безопасности.
17. Работа с документами в области информационной безопасности РФ по определению объектив защиты и классификации тайн
18. Определение объектов защиты на типовом объекте информатизации
19. Классификация защищаемой информации по видам тайны и степеням конфиденциальности
20. Понятие угрозы безопасности информации.
21. Системная классификация угроз безопасности информации.

22. Каналы и методы несанкционированного доступа к информации.
23. Уязвимости. Методы оценки уязвимости информации
24. Анализ существующих методик определения требований к защите информации.
25. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
26. Виды мер и основные принципы защиты информации.
27. Организационная структура системы защиты информации.
28. Законодательные акты в области защиты информации.
29. Российские и международные стандарты, определяющие требования к защите информации.
30. Система сертификации РФ в области защиты информации.
31. Основные правила и документы системы сертификации РФ в области защиты информации
32. Основные механизмы защиты информации.
33. Система защиты информации.
34. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
35. Программные и программно-аппаратные средства защиты информации
36. Инженерная защита и техническая охрана объектов информатизации
37. Организационно-распорядительная защита информации.
38. Работа с кадрами и внутриобъектовый режим.
39. Принципы построения организационно-распорядительной системы.

КРИТЕРИИ ОЦЕНКИ

Критерии оценки ответа, экзаменующегося:

оценка «5»	– полностью раскрыто содержание материала в объеме, предусмотренном программой; – изложен материал грамотным языком в определенной логической последовательности, точно используя специализированную терминологию и символику; – правильно выполнено графическое изображение, схема, модель, программа, сопутствующие ответу
оценка «4»	– ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: – в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа; – допущены ошибка или более двух недочетов в графическом представлении материала.
оценка «3»	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, моделях, блок-схем, графиков.
оценка «2»	– не раскрыто основное содержание материала; – обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала, – допущены ошибки в определении понятий, при использовании терминологии, в моделях, блок-схемах, графиках

Дополнительно членами комиссии при оценивании обучающегося учитываются:

Показатели оценки результата	**Оценка (да /**

	нет)
Грамотность речи при устном обосновании материала	
Аргументированность изложения материала	
Соблюдение регламента ответов	
Способность проявлять ответственность за результат выполнения задания	
Грамотность использования ИКТ при выборе материала	
Соблюдение профессиональной этики при ответе	

3. ЛИСТ СОГЛАСОВАНИЯ

Дополнения и изменения к комплекту КОС

Дополнения и изменения к комплекту КОС на_____учебный год по дисциплине _____

В комплект КОС внесены следующие изменения:

_____

_____

_____

_____

_____

Дополнения и изменения в комплекте КОС обсуждены на заседании предметной цикловой комиссии информационной безопасности телекоммуникационных систем

«____»_____20_____г. (протокол №_____).

Председатель ЦК _____ Н.В. Кривоносова