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

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

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

ЗАЩИТА ИНФОРМАЦИИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАМНЫХ И ПРОГРАММНО-АППАРАТНЫХ (В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ ЗАЩИТЫ

(наименование профессионального модуля)

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 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием програмных и программно-аппаратных, в (том числе криптографических) средств защиты»

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

Оглавление

1. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Вид деятельности

Результатом освоения профессионального модуля является освоение вида деятельности Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты:

В результате освоения программы профессионального модуля у обучающихся должны быть сформированы следующие компетенции, получены знания и развиты умения:

Таблица 1

Код компетенции	Содержание компетенции	Показатели оценки результата (знания, умения)
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Умения: – распознавать задачу и/или проблему в профессиональном и/или социальном контексте; – анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; – выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; – составить план действия; – определить необходимые ресурсы; – владеть актуальными методами работы в профессиональной и смежных сферах; – реализовать составленный план; – оценивать результат и последствия своих действий (самостоятельно или с помощью наставника). Знания: – актуальный профессиональный и социальный контекст, в котором приходится работать и жить; – основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; – алгоритмы выполнения работ в профессиональной и смежных областях; – методы работы в профессиональной и смежных сферах; – структуру плана для решения задач; – порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для	Умения: – определять задачи для поиска информации; – определять необходимые источники информации; – планировать процесс поиска;

	выполнения задач профессиональной деятельности	– структурировать получаемую информацию; – выделять наиболее значимое в перечне информации; – оценивать практическую значимость результатов поиска; – оформлять результаты поиска. Знания: – номенклатура информационных источников, применяемых в профессиональной деятельности; – приемы структурирования информации; – формат оформления результатов поиска информации.
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 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Умения: – организовывать работу коллектива и команды; – взаимодействовать с коллегами, руководством, клиентами. Знания: – психология коллектива; – психология личности; – основы проектной 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	Умения: – понимать общий смысл четко произнесенных высказываний на известные темы

	государственном и иностранных языках.	(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

Код ПК	**Наименование компетенции**
ПК 2.1	Производить 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.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

Таблица 3

Уметь:	
У-1	выявлять и оценивать угрозы безопасности информации в ИТКС;
У-2	настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
У-3	проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
У-4	проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
У-5	проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

У-6	проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
У-7	проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.
Знать:	
З-1	возможные угрозы безопасности информации в ИТКС;
З-2	способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
З-3	типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
З-4	криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
З-5	порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
З-6	организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
З-7	порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

В результате освоения программы профессионального модуля обучающийся должен иметь практический опыт:

Таблица 4

Практический опыт:	
ПО-1	установка, настройка, испытания и конфигурирование программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
ПО-2	поддержание бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
ПО-3	защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

1.2. Матрица компетенций ПМ 02

Элемент КОС	**Проверяемые общие и профессиональные компетенции (знания, умения), практический опыт**																								
	ОК 01	ОК 02	ОК 03	ОК 04	ОК 09	ОК 10	У - 1	У - 2	У - 3	У - 4	У - 5	У - 6	У - 7	З - 1	З - 2	З - 3	З - 4	З - 5	З - 6	З - 7	ПО - 1	ПО - 2	ПО - 3	ПК 2.1	ПК 2.2	ПК 2.3
МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты																										
ЛР 1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

ЛР 6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 9	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 10	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 11	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 12	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 13	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 16	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 17	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 18	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+	+		+	+	+	+
ПЗ 1	+	+	+	+	+	+	+	+						+	+	+	+	+	+	+	+			+	+
ПЗ 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+
ПЗ 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+
ПЗ 8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+
ПЗ 9	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 10	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 11	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 12	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 13	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
МДК 02.02 Криптографическая защита информации																									
ЛР 1	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 2	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 3	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 4	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 5	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+

ЛР 6	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 7	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 8	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ЛР 9	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЛР 10	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 1	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+		+	+	+	+
ПЗ 2	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+		+	+	+	+
ПЗ 3	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+		+	+	+	+
ПЗ 4	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+		+	+	+	+
ПЗ 5	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 6	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 7	+	+	+	+	+	+	+	+	+	+				+	+	+	+	+	+	+		+	+	+	+
ПЗ 8	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+		+	+	+	+
ПЗ 9	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 10	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 11	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПЗ 12	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Описание лабораторных и практических работ см. – Методические указания по выполнению практических работ; Методические указания по выполнению лабораторных работ.

2. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Обязательной формой аттестации по итогам освоения программы профессионального модуля являются дифференцированный зачет по МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты ,МДК 02.02 Криптографическая защита информации, прохождение учебной и производственной практик, экзамен (квалификационный). Результатом экзамена является однозначное решение: «вид деятельности освоен / не освоен».

2.1. Запланированные формы промежуточной аттестации по ПМ.02

Таблица 5

Элементы модуля, профессиональный модуль	**Формы промежуточной аттестации**
МДК 02.01	*Дифференцированный зачёт*
МДК 02.02	*Дифференцированный зачёт*
Учебная практика	*Дифференцированный зачёт*
Производственная практика	*Дифференцированный зачёт*
ПМ.02	*Экзамен*

3. ОЦЕНКА ОСВОЕНИЯ ТЕОРЕТИЧЕСКОГО КУРСА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Основной целью оценки курса профессионального модуля является оценка приобретенных умений, знаний и компетенций.

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;
  - защита курсовых проектов (работ);
  - прием индивидуальных домашних заданий, рефератов, отчетов по лабораторным работам.

Текущий контроль обеспечивают выполнение видов работ на практике, освоение тем, выполнение лабораторных/практических работ, выполнение самостоятельных работ по МДК 02.01 и МДК 02.02.

Таблица 6

ПК 2.1. Производить 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.	
Иметь практический опыт:	***Виды работ на практике:***
– установка, настройка, испытания и конфигурирование программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС; – поддержание бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС; – защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.	– работа с учетными записями пользователей; – настройка параметров безопасности ОС; – управление хранением данных; – архивация данных; – восстановление данных; – аудит ресурсов ОС; – аудит событий ОС; – управление доступом в Linux; – управление доступом в Windows; – средства аутентификации операционных систем; – управление средствами аутентификации Linux; – управление средствами аутентификации Windows.
Уметь:	***Тематика лабораторных/практических работ:***

– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; – проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.	– средства идентификации аутентификации операционных систем; – настройка локальной политики безопасности операционной системы. Политика паролей. Политики учетных записей; – назначение прав пользователя; – настройка изолированной среды; – параметры безопасности. Политика аудита; – АПМДЗ Криптон: инициализация системного администратора, инициализация пользователя, проверка целостности среды; – аппаратные средства шифрования Криптон: настройка, эксплуатация; – программные средства шифрования. Защищенные контейнеры; – восстановление информации типовыми средствами; – программы надежного удаления информации; – архивирование информации; – программные средства резервного копирования. Настройка RAID-массивов; – инсайдерская информация. Программы сбора информации о ПК; – примеры политик безопасности VPN; – протоколы защиты данных канального уровня (PPTP, L2F и L2TP). Сравнительный анализ протоколов защиты на канальном уровне; – защита данных на сетевом уровне (Протокол IPSec). Протоколы туннельного и транспортного режимов; – защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS); – инфраструктура открытых ключей (ИОК). Модели APKI и PKIX – сертификат открытого ключа. Формат сертификации открытого ключа. Аннулирование сертификатов; – реализация алгоритмов скоростной криптозащиты; – VPN на базе сетевых операционных систем; – VPN на базе специализированного программного обеспечения; – VPN на базе аппаратных средств; – использование токена на рабочем месте администратора; – установка и настройка СКЗИ «КриптоПро CSP»;

	– работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP
Знать:	***Перечень тем, включенных в МДК:***
– возможные угрозы безопасности информации в ИТКС; – способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё; – типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; – криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; – порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; – организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; – порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.	**Тема 1.1. Обеспечение безопасности операционных систем** **Тема 1.2. Технологии разграничения доступа** **Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN**
Самостоятельная работа	работа с конспектами, литературой; подготовка отчетов практических работ
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации информационно-телекоммуникационных системах и сетях	
Иметь практический опыт:	***Виды работ на практике:***
– установка, настройка, испытания и конфигурирование программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;	– документирование политики безопасности; – выбор, подключение, настройка межсетевого экрана, – администрирование межсетевого экрана; – ознакомление, подключение, настройка системы резервного копирования;

– поддержание бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС; – защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.	– администрирование системы резервного копирования; – ознакомление, подключение, настройка системы антивирусной защиты; – администрирование системы антивирусной зашиты; – изучение методов комплексного исследования объекта информатизации; – изучение информации циркулирующей в корпоративной информационной системе; – изучение построения системы защиты информации на основе нормативных актов и методических указаний.
Уметь:	***Тематика лабораторных/практических работ:***
– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; – проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.	– настройка межсетевого экрана; – конфигурация правила для СОВ; – развертывание открытых списков правил; – подключение средства мониторинга; – включение режима блокировки; – проектирование стенда для реализации IDS; – настройка интерфейсов виртуальных машин; – стеганографические методы скрытия информации; – применение методов шифрования перестановкой; – применение методов шифрования заменой; – применение методов шифрования многоалфавитной замены; – криптоанализ методов перестановки; – криптоанализ методов замены; – компьютерное шифрование – проектирование стенда для реализации IDS
Знать:	***Перечень тем, включенных в МДК:***

– возможные угрозы безопасности информации в ИТКС; – способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё; – типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; – криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; – порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; – организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; – порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.	**Тема 1.4. Технологии обнаружения вторжений** **Тема 1.5. Методы управления средствами защиты** **Тема 2.1. Основы криптографических методов защиты информации**
Самостоятельная работа	работа с конспектами, литературой; подготовка отчетов практических работ
ПК 2.3. Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями	
Иметь практический опыт:	***Виды работ на практике:***
– установка, настройка, испытания и конфигурирование программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС; – поддержание бесперебойной работы программных и программно-аппаратных в том	– построение модели угроз ИСПДн; – определение вероятности реализации угроз безопасности в информационной системе персональных данных; – изучение действующей нормативной документации объекта информатизации; – составление плана мероприятий по улучшению защищенности объекта информатизации;

числе криптографических средств защиты информации в ИТКС; – защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.	– разработка КСЗИ информационной системы: сбор данных; – разработка КСЗИ информационной системы: выбор технологий; – разработка КСЗИ информационной системы: разработка модели; – разработка КСЗИ информационной системы: оформление решений.
Уметь:	***Тематика лабораторных/практических работ:***
– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; – проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; – проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.	– алгоритм Диффи-Хелмана; – стандарт симметричного шифрования AES RIJNDAEL; – генерация простых чисел, используемых в асимметричных системах шифрования;криптографические хэш-функции. Аутентификация; – шифрование методом скользящей перестановки; – изучение программных продуктов защиты информации. Программа PGP (Pretty Good Privacy); – шифр Плейфера; – Российский стандарт хэш-функции ГОСТ Р 34.11-94 – криптосистема RSA; – электронная цифровая подпись; – разработка схемы простого пароля; – разработка схемы динамического пароля; – сертификаты открытого ключа; – настройка и администрирование токена – настройка сервисов Рутокен
Знать:	***Перечень тем, включенных в МДК:***
– возможные угрозы безопасности информации в ИТКС; – способы защиты информации от несанкционированного доступа	**Тема 2.2. Современные стандарты шифрования** **Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий**

(далее – НСД) и специальных воздействий на неё; – типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; – криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; – порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; – организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; – порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.	
Самостоятельная работа	работа с конспектами, литературой; подготовка отчетов практических работ

3.1. Типовые задания для оценки освоения МДК 02.01, МДК 02.02 текущий, промежуточная аттестация (тесты/задания)

Текущий контроль осуществляется за счет выполнения практических и самостоятельных работ, описание которых даны в методических рекомендациях по выполнению ЛПР по МДК 04.00 и в методических рекомендациях по выполнению ВСР.

3.1.1. Тестовые вопросы для промежуточной аттестации по Теме 1.1. Обеспечение безопасности операционных систем

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Вредоносная программа, распространяющаяся по сети и самовоспроизводящаяся -	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

2	Вирус, который подсоединяется к обычной программе или данным -	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Какие вирусы активизируются в самом начале работы с операционной системой:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Наиболее защищенная файловая система – это:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Комплекс мероприятий, которые направлены на защиту информации:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	проверка целостности и подлинности информации, программы, документа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Кто в компании является основным ответственным за определение уровня классификации информации?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Какой перехват осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера?	ПК 2.1 ПК 2.2 ПК 2.3	30

		ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
9	Какие из средств защиты информации направлены на защиту оборудования?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Как называется состояние информационной среды, в котором обеспечены конфиденциальность, целостность и доступность информации?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Основными источниками угроз информационной безопасности являются все указанное в списке: 1. Хищение жестких дисков, подключение к сети, инсайдерство; 2. Перехват данных, хищение данных, изменение архитектуры системы; 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Виды информационной безопасности: 1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	В чем суть атаки типа переполнение буфера? 1. порча памяти другого процесса из-за отсутствия контроля границ буфера; 2. переполнение памяти компьютерной системы ; 3. перезагрузка ОС ; 4. нарушение правильности ввода-вывода;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	В чем суть тестирования на безопасность? 1. тестирование на стрессовые нагрузки;	ПК 2.1 ПК 2.2	30

	2. тестирование на случайные данные; 3. имитация атакующих действий хакеров и проверка подсистемы безопасности на защиту от них.	ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
5	Основная масса угроз информационной безопасности приходится на: 1. Троянские программы; 2. Шпионские программы; 3. Черви.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Под какие системы распространение вирусов происходит наиболее динамично: 1. Windows 2. Mac OS 3. Android	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Заключительным этапом построения системы защиты является: 1. сопровождение 2. планирование 3. анализ уязвимых мест	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Конфиденциальностью называется: 1. защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов 2. защита от несанкционированного доступа к информации 3. описание процедур	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности: 1. хакеры; 2. контрагенты; 3. сотрудники.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Какие угрозы безопасности информации являются преднамеренными: 1. ошибки персонала 2. открытие электронного письма, содержащего вирус	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02	30

	3. не авторизованный доступ	ОК 03 ОК 04 ОК 09 ОК 10	

3.1.2. Тестовые вопросы для промежуточной аттестации по Теме 1.2. Технология разграничения доступа

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Для чего используется система Kerberos?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Агрессивное потребление ресурсов является угрозой:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Возможность за приемлемое время получить требуемую информационную услугу называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Сколько уровней включает в себя сетевая модель OSI?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	На каком уровне сетевой модели OSI не работает межсетевой экран:	ПК 2.1	30

		ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
7	небольшое количество дополнительной цифровой информации, передаваемое вместе с подписываемым текстом, по которому можно удостоверится в аутентичности документа - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	IP адрес имеет длину	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Ключ, доступный всем для проверки цифровой подписи под документом	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	В качестве аутентификатора в сетевой среде могут использоваться: 1. год рождения субъекта; 2. фамилия субъекта; 3. секретный криптографический ключ.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09	30

		ОК 10	
2	В число основных понятий ролевого управления доступом входит: 1. роль 2. исполнитель роли; 3. пользователь роли;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	В число основных понятий ролевого управления доступом входит: 1. субъект; 2. объект; 3. метод.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Ролевое управление доступом использует следующее средство объектно-ориентированного подхода: 1. инкапсуляция; 2. полиморфизм; 3. наследование.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	При использовании сервера аутентификации Kerberos пароли по сети: 1. не передаются; 2. передаются в зашифрованном виде; 3. передаются в открытом виде.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Сервер аутентификации Kerberos: 1. не защищает от атак на доступность; 2. частично защищает от атак на доступность; 3. полностью защищает от атак на доступность.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	К какому типу протоколов относится протокол SSL? 1. К протоколам прямой аутентификаци 2. К протоколам автономной аутентификации 3. К протоколам установления защищенной связи на сетевом уровне 4. К протоколам непрямой аутентификации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Что понимается под затенением файла с паролями пользователей?	ПК 2.1 ПК 2.2	30

	1. Запрет доступа к файлу для непривилегированных пользователей 2. Перенос на защищенный от несанкционированного чтения носитель 3. Замена * символов паролей 4. Запрет доступа к файлу для любых процессов	ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
9	Что относится к локальному уровню правового регулирования информационной безопасности? 1. Принятие государственных стандартов 2. Принятие постановлений правительства 3. Утверждение перечня сведений, составляющих коммерческую тайну 4. Принятие федеральных законов	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Что не может использоваться при биометрической аутентификации? 1. Отпечатки пальцев 2. Температура тела 3. Геометрическая форма руки 4. Тембр голоса	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.3. Тестовые вопросы для промежуточной аттестации по Теме 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN.

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра -	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран, является недостатком VPN на основе…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним – это …	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03	30

		ОК 04 ОК 09 ОК 10	
4	В ходе выполнения процедуры … происходит подтверждение валидности пользователя	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Какая топология представлена на рисунке?  	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	устройства, с помощью которых можно выявлять и своевременно предотвращать вторжения в вычислительные сети	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	…определяет виртуальную частную сеть	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Метод, позволяющий воспользоваться общедоступной телекоммуникационной инфраструктурой для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Верно ли, что VPN и беспроводные технологии не конкурируют, а дополняют друг друга	ПК 2.1 ПК 2.2 ПК 2.3	30

		ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
10	При использовании топологии … удаленные пользователи подключаются к корпоративной сети через Internet	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Неверно, что статистические методы анализа могут быть применены ... 1. при значительном (более 1000) числе рабочих мест сети 2. при отсутствии шаблонов типичного поведения в распределенных сетях	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Основное отличие активного радиочастотного идентификатора от пассивного в ... 1. наличии блока питания 2. способности излучать радиосигнал 3. особенностях архитектуры ЗУ	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Высокая стоимость решения в пересчете на одно рабочее место является недостатком VPN на основе … 1. маршрутизаторов 2. межсетевых экранов 3. программных решений	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Обнаружение вирусов, ранее не известных, возможно при использовании … 1. метода сравнения с эталоном эвристического анализа 2. антивирусного мониторинга 3. метода обнаружения изменений	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	VPN определяет:	ПК 2.1	30

	1. базовую станцию беспроводной сети 2. сервер проводной сети Ethernet 3. виртуальную частную сеть	ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
6	Виртуальная частная сеть - это метод, позволяющий: 1. посредством беспроводной сети Wi-Fi организовать более безопасное соединение между всеми компонентами сети 2. воспользоваться общедоступной телекоммуникационной инфраструктурой для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации 3. обычным пользователям, не подключенным к Wi-Fi сети, обмениваться информацией через Internet	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Безопасность VPN-сетей включает в себя: 1. защиту соединения между хостами в беспроводной локальной сети 2. защиту информации каждого пользователя в сети 3. развертывание информационных услуг посредством функций сети	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Основное достоинство конфигурации "сеть-сеть" состоит в том, что: 1. сети выглядят как смежные, а работа VPN-шлюзов прозрачна для пользователей 2. работа VPN-шлюзов не доступна пользователям 3. полная незащищенность сети	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	IPSec определяет: 1. метод взаимодействия пользователей с VPN 2. наиболее широко признанный, поддерживаемый и стандартизованный из всех протоколов VPN 3. протокол управления содержимым. Почти не используется в VPN	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	ESP определяет: 1. безопасно инкапсулированную полезную нагрузку 2. заголовок аутентификации 3. схему обмена ключами через Internet	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.4. Тестовые вопросы для промежуточной аттестации по Теме 1.4. Технологии обнаружения вторжений

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Шаблон вредоносной активности называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Программное или аппаратное средство предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления или в основном через Интернет это -…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Как по - другому называется анализатора трафика?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Верно ли, что системы обнаружения вторжений бывают комбинированными, сетевыми и хостовыми?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

7	Большинство систем обнаружения вторжений группируют сигналы тревоги по:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	В пассивной системе обнаружения вторжений при обнаружении нарушений безопасности, информация о нарушении записывается в…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Протокольные СОВ используются для….	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Основным методом, применяемым в сетевых системах обнаружения вторжений, является исследование проходящего трафика и: 1. ввод полученных данных в самообучающиеся нейронные сети; 2. сравнение его с базой данных известных шаблонов вредоносной активности; 3. сравнение его статистических характеристик с профилями нормальной активности	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Основным методом, применяемым в хостовых системах обнаружения вторжений, является: 1. контроль целостности ключевых файлов 2. сравнение статистических характеристик поведения пользователей с профилями нормальной активности 3. сравнение статистических характеристик поведения программ	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04	30

	с профилями нормальной активности	ОК 09 ОК 10	
3	Ложное срабатывание сетевой системы обнаружения вторжений имеет место, когда: 1. система генерирует сигнал тревоги на основе того, что она считает вредоносной или подозрительной активностью, но что в действительности оказывается нормальным трафиком для данной сети 2. система не срабатывает, пропуская неизвестную атаку 3. система не успевает анализировать трафик в реальном масштабе времени	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	К числу типичных причин ложных срабатываний сетевых систем обнаружения вторжений принадлежат: 1. максимальная подозрительность подразумеваемой конфигурации 2. максимальная подозрительность подразумеваемой конфигурации 3. отсутствие обновлений в подразумеваемой конфигурации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Чтобы минимизировать число ложных срабатываний системы обнаружения вторжений, следует: 1. минимизировать число настраиваемых параметров 2. использовать подразумеваемые настройки 3. индивидуализировать настройки для своей сети	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Категорию сигналов тревоги для UNIX-платформ можно безопасно отключить, если: 1. в сети нет UNIX-систем 2. вы уверены в безопасности UNIX-систем 3. длительное время не генерируются сигналы тревоги для UNIX-систем	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Лучшим способом обработки сигналов тревоги является: 1. их немедленное занесение в базу данных 2. отправка сообщения по электронной почте 3. протоколирование для последующего просмотра	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Для систем обнаружения вторжений имеются средства анализа: 1. только коммерческие программные средства 2. с открытыми исходными текстами 3. не существует программных средств анализа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

9	Сетевые системы обнаружения вторжений желательно запускать на: 1. одном компьютере с межсетевым экраном 2. одном компьютере с общедоступным сервисом 3. специально выделенном компьютере	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Размещение сетевой системы обнаружения вторжений в ЛВС позади межсетевого экрана позволяет: 1. прослушивать локальную среду передачи 2. прослушивать среду передачи в демилитаризованной зоне 3. прослушивать среду передачи перед межсетевым экраном	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.5. Тестовые вопросы для промежуточной аттестации по Теме 1.5. Методы управления средствами защиты

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Административные действия в СУБД позволяют выполнять привилегии	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Восстановление данных является дополнительной функцией услуги защиты	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02	30

		ОК 03 ОК 04 ОК 09 ОК 10	
5	Единственный ключ используется в _____ криптосистемах	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Запись определенных событий в журнал безопасности сервера называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Наиболее надежным механизмом для защиты содержания сообщений является:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Применение услуги причастности рекомендуется на _____ уровне модели OSI	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09	30

		ОК 10	

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Риски в сфере информационной безопасности разделяются на: 1. внешние и внутренние 2. объективные и субъективные 3. системные и операционные	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Меры информационной безопасности направлены на защиту от: 1. нанесения неприемлемого ущерба; 2. нанесения любого ущерба 3. подглядывания в замочную скважину	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует: 1. область равного доступа; 2. уровень безопасности 3. уровень доступности	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	С помощью закрытого ключа информация: 1. копируется 2. транслируется 3. расшифровывается 4. зашифровывается	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется: 1. актуальностью информации 2. доступностью 3. качеством информации 4. целостностью	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Согласно «Оранжевой книге» уникальные идентификаторы должны иметь: 1. наиболее важные субъекты 2. наиболее важные объекты 3. все субъекты	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02	30

	4. все объекты	ОК 03 ОК 04 ОК 09 ОК 10	
7	Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это: 1. уязвимость информации 2. надежность информации 3. защищенность информации 4. базопасность информации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Наименее затратный криптоанализ для криптоалгоритма DES 1. перебор по выборочному ключевому пространству 2. разложение числа на сложные множители 3. перебор по всему ключевому пространству 4. разложение числа на простые множители	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	К основным функциям системы безопасности можно отнести все перечисленное: 1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: 1. Регламентированной 2. Правовой 3. Защищаемой	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.6. Тестовые вопросы для промежуточной аттестации по Теме 2.1. Основы криптографических методов защиты информации

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Преобразование понятного текста в зашифрованный с целью защиты информации - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Слово "криптография" произошло от	ПК 2.1	30

		ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
3	Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Как называется процесс наложения по определенному закону гамма-шифра на открытые данные	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Как называется криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называется	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод …	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01	30

		ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
9	Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	В чем суть метода открытого и скрытого ключей? 1. криптование скрытым ключом и декриптование открытым ключом; 2. использование суммы двух ключей в качестве ключа для криптования; 3. криптование открытым ключом и декриптование скрытым ключом.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства? 1. шифр Маркова 2. шифр Цезаря 3. шифр Энигма 4. шифр Бэбиджа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты? 1. Алгоритм 2. Ключ 3. Протокол 4. Шифр	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Как называется сообщение, полученное после преобразования с использованием любого шифра?	ПК 2.1 ПК 2.2	30

	1. закрытым текстом 2. имитовставкой 3. ключом	ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
5	Что в криптографии называют открытым текстом? 1. исходное сообщение (сообщение до шифрования) 2. открытый ключ шифрования 3. сообщение, получение после преобразования с использованием любого шифра 4. электронную цифровую подпись	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Какая наука разрабатывает методы «вскрытия» шифров? 1. Криптография 2. Криптоанализ 3. Тайнопись	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Что такое криптостойкость? 1. характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа 2. свойство гаммы 3. все ответы верны	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности? 1. алгоритмом гаммирования 2. алгоритмом перестановки 3. алгоритмом аналитических преобразований	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера: 1. 4 2. 3 3. 5	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Суть метода перестановки: 1. символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов 2. замена алфавита	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02	30

	3. все правильные	ОК 03 ОК 04 ОК 09 ОК 10	

3.1.7. Тестовые вопросы для промежуточной аттестации по Теме 2.2. Современные стандарты шифрования

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	На сколько блоков будет разбито сообщение размером 1 Кбайт для шифрования алгоритмом DES?Ответ запишите в виде одного числа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Как называется способ шифрования, в котором шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	функция, которая для строки произвольной длины вычисляет некоторое характерное целое значение или некоторую другую строку фиксированной длины	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Сколько ключей используется в криптографических алгоритмах с открытым ключом?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Относится ли алгоритм DES к алгоритмам шифрования с открытым ключом?	ПК 2.1 ПК 2.2	30

		ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
7	Верно ли утверждение: «алгоритм RC4 можно использовать для генерации псевдослучайной ключевой последовательности при поточном шифровании информации»?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Верно ли утверждение: «поточные шифры применяются для формирования электронной цифровой подписи»?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Как называется сообщение, полученное после преобразования с использованием любого шифра?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней: 1. шифрование 2. зашифровка 3. закрытость	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

2	Алгоритм DES является 1. алгоритмом вычисления функции хеширования 2. алгоритмом формирования электронной цифровой подписи 3. блочным алгоритмом асимметричного шифрования 4. блочным алгоритмом симметричного шифрования	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Как называется комбинация нескольких подряд примененных простых шифров, дающих в результате более сложное преобразование? 1. асимметричный шифр 2. последовательный шифр 3. композиционный шифр 4. сложный шифр	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Как расшифровывается аббревиатура DES? 1. Data Extended Standard 2. Deep Extended Standard 3. Deep Encryption Standard 4. Data Encryption Standard	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Как расшифровывается аббревиатура AES? 1. Advanced Encryption Standard 2. Analytic Encryption Standard 3. American Extended Standard 4. Advanced Extended Standard	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Как называется режим использования блочного шифра, в котором каждый блок исходных данных шифруется независимо от остальных блоков с применением одного и того же ключа шифрования? 1. режим простой поблочной замены 2. режим сцепления блоков шифра 3. режим формирования электронной цифровой подписи 4. режим создания хеш-кода	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Как называется режим использования блочного шифра, в котором перед шифрованием каждый блок открытого текста складывается по модулю 2 с результатом шифрования предыдущего блока? 1. режим простой поблочной замены 2. режим сцепления блоков шифра 3. режим формирования электронной цифровой подписи	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Алгоритм DES является 1. алгоритмом вычисления функции хеширования 2. алгоритмом формирования электронной цифровой подписи	ПК 2.1 ПК 2.2 ПК 2.3	30

	3. блочным алгоритмом асимметричного шифрования 4. блочным алгоритмом симметричного шифрования	ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
9	Как называется однозначное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? 1. Хеширование 2. Гаммирование 3. Перестановка	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	На чем основана безопасность алгоритма RSA для формирования цифровой подписи? 1. на трудности возведения целых чисел в степень по модулю 2. на трудности вычисления дискретных логарифмов 3. на трудности решения задачи факторизации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.8. Тестовые вопросы для промежуточной аттестации по Теме 2.3. Криптографические методы обеспечения безопасности сетевых технологий

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	попытка получения злоумышленником информации, для просмотра которой у него нет разрешений - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	потенциальный путь для выполнения атаки – это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09	30

		ОК 10	
4	механизм аутентификации, предполагающий использование определенного устройства для идентификации человеческих характеристик	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	На каком уровне модели OSI осуществляется маршрутизация?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Какие системы предназначены для обеспечения сетевого мониторинга, анализа и оповещения в случае обнаружения сетевой атаки?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Как называется процедура предоставления определенному пользователю прав на выполнение некоторых действий?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Что такое IPTV?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	На каком уровне модели OSI создают туннели протоколы L2TP и PPTP?	ПК 2.1 ПК 2.2	30

		ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	

Часть 2

№	Вопрос	Ответ	ОК/ПК	Время, сек
1	Порт 80 позволяет: 1. осуществлять доступ к веб 2. передавать файлы 3. получать и отсылать почту	1	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Что является основной причиной распространения использования беспроводных технологий? 1. недорогой метод соединения информационных систем 2. высокая скорость передачи данных 3. высокая защищенность соединений	1	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Данная политика определяет степень секретности информации внутри организации и необходимые требования к хранению, передаче, пометке и управлению этой информацией. 1. политика безопасности 2. информационная политика 3. политика резервного копирования	1	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Сколько интерфейсов у межсетевого экрана прикладного уровня? 1. 1 2. 2 3. по одному на каждую сеть, к которым он подключен	3	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Для защиты от атак какого типа предназначена служба конфиденциальности? 1. атаки доступа 2. атаки модификации 3. атаки отказа в обслуживании	1	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Какое назначение службы DNS?	2	ПК 2.1	30

	1. синхронизация времени 2. разрешения системных имен и их преобразования в IP адреса 3. поддержка функционирования сети		ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
7	Какие требования предъявляются к корневому каталогу веб-сервера? 1. не должен совпадать с системным корневым каталогом 2. не должен превышать 2 Гбайт 3. должен содержать файл index.html (index.php)	1	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Межсетевой экран 1. защищает внутренние сети от внешних атак 2. обеспечивает защиту от злоумышленника, использующего для входа в систему законную программу 3. обеспечивает защиту, если злоумышленник через уязвимые места получит доступ к файлам как администратор	1	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Как называется стандарт для виртуальных локальных сетей? 1. IEEE 802.11 2. IEEE 802.11i 3. IEEE 802.1Q	3	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	192.168.1.1 – это … 1. MAC-адрес 2. SSID 3. IP-адрес в IPv4	3	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.9. Тестовые вопросы для промежуточной аттестации МДК 02.01
Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Вирус, который подсоединяется к обычной программе или данным -	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04	30

		ОК 09 ОК 10	
2	Какие вирусы активизируются в самом начале работы с операционной системой:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Наиболее защищенная файловая система – это:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Агрессивное потребление ресурсов является угрозой:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Сколько уровней включает в себя сетевая модель OSI?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Какие из средств защиты информации направлены на защиту оборудования?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Как называется состояние информационной среды, в котором обеспечены конфиденциальность, целостность и доступность информации?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Доступ субъекта к объекту в нарушение установленных в системе	ПК 2.1	30

	правил разграничения доступа - это	ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
9	IP адрес имеет длину	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Ключ, доступный всем для проверки цифровой подписи под документом	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
11	Зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран, является недостатком VPN на основе…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
12	Сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним – это …	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
13	В ходе выполнения процедуры … происходит подтверждение валидности пользователя	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
14	Какая топология представлена на рисунке?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01	30

		ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
15	Верно ли, что VPN и беспроводные технологии не конкурируют, а дополняют друг друга	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
16	Шаблон вредоносной активности называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
17	Программное или аппаратное средство предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления или в основном через Интернет это -…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
18	Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к…	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
19	…определяет виртуальную частную сеть	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

20	метод, позволяющий воспользоваться общедоступной телекоммуникационной инфраструктурой для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
21	Как по - другому называется анализатора трафика?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
22	Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
23	Верно ли, что системы обнаружения вторжений бывают комбинированными, сетевыми и хостовыми?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
24	Большинство систем обнаружения вторжений группируют сигналы тревоги по:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
25	процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
26	устройства, с помощью которых можно выявлять и своевременно предотвращать вторжения в вычислительные сети	ПК 2.1 ПК 2.2 ПК 2.3	30

		ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
27	Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
28	IP адрес имеет длину	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
29	Ключ, доступный всем для проверки цифровой подписи под документом	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
30	Как называется состояние информационной среды, в котором обеспечены конфиденциальность, целостность и доступность информации?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Основными источниками угроз информационной безопасности являются все указанное в списке: 1. Хищение жестких дисков, подключение к сети, инсайдерство; 2. Перехват данных, хищение данных, изменение архитектуры системы; 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Виды информационной безопасности:	ПК 2.1	30

	1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
3	В чем суть атаки типа переполнение буфера? 1. порча памяти другого процесса из-за отсутствия контроля границ буфера; 2. переполнение памяти компьютерной системы ; 3. перезагрузка ОС ; 4. нарушение правильности ввода-вывода;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	В чем суть тестирования на безопасность? 1. тестирование на стрессовые нагрузки; 2. тестирование на случайные данные; 3. имитация атакующих действий хакеров и проверка подсистемы безопасности на защиту от них.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Основная масса угроз информационной безопасности приходится на: 1. Троянские программы; 2. Шпионские программы; 3. Черви.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Ролевое управление доступом использует следующее средство объектно-ориентированного подхода: 1. инкапсуляция; 2. полиморфизм; 3. наследование.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Под какие системы распространение вирусов происходит наиболее динамично: 1. Windows; 2. Mac OS; 3. Android.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Заключительным этапом построения системы защиты является: 1. Сопровождение; 2. планирование;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01	30

	3. анализ уязвимых мест.	ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
9	В качестве аутентификатора в сетевой среде могут использоваться: 1. год рождения субъекта; 2. фамилия субъекта; 3. секретный криптографический ключ.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	В число основных понятий ролевого управления доступом входит: 1. роль 2. исполнитель роли; 3. пользователь роли;	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
11	В число основных понятий ролевого управления доступом входит: 1. субъект; 2. объект; 3. метод.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
12	Сервер аутентификации Kerberos: 1. не защищает от атак на доступность; 2. частично защищает от атак на доступность; 3. полностью защищает от атак на доступность.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
13	К какому типу протоколов относится протокол SSL? 1. К протоколам прямой аутентификаци 2. К протоколам автономной аутентификации 3. К протоколам установления защищенной связи на сетевом уровне 4. К протоколам непрямой аутентификации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
14	Что понимается под затенением файла с паролями пользователей? 1. Запрет доступа к файлу для непривилегированных пользователей 2. Перенос на защищенный от несанкционированного чтения носитель 3. Замена * символов паролей	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04	30

	4. Запрет доступа к файлу для любых процессов	ОК 09 ОК 10	
15	Что относится к локальному уровню правового регулирования информационной безопасности? 1. Принятие государственных стандартов 2. Принятие постановлений правительства 3. Утверждение перечня сведений, составляющих коммерческую тайну 4. Принятие федеральных законов	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
16	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности: 1. хакеры; 2. контрагенты; 3. сотрудники.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
17	Какие угрозы безопасности информации являются преднамеренными: 1. ошибки персонала 2. открытие электронного письма, содержащего вирус 3. не авторизованный доступ	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
18	Неверно, что статистические методы анализа могут быть применены ... 1. при значительном (более 1000) числе рабочих мест сети 2. при отсутствии шаблонов типичного поведения в распределенных сетях	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
19	Основное отличие активного радиочастотного идентификатора от пассивного в ... 1. наличии блока питания 2. способности излучать радиосигнал 3. особенностях архитектуры ЗУ	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
20	Высокая стоимость решения в пересчете на одно рабочее место является недостатком VPN на основе … 1. маршрутизаторов 2. межсетевых экранов 3. программных решений	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
21	Обнаружение вирусов, ранее не известных, возможно при	ПК 2.1	30

	использовании … 1. метода сравнения с эталоном эвристического анализа 2. антивирусного мониторинга 3. метода обнаружения изменений	ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
22	Основным методом, применяемым в сетевых системах обнаружения вторжений, является исследование проходящего трафика и: 1. ввод полученных данных в самообучающиеся нейронные сети; 2. сравнение его с базой данных известных шаблонов вредоносной активности; 3. сравнение его статистических характеристик с профилями нормальной активности	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
23	Основным методом, применяемым в хостовых системах обнаружения вторжений, является: 1. контроль целостности ключевых файлов 2. сравнение статистических характеристик поведения пользователей с профилями нормальной активности 3. сравнение статистических характеристик поведения программ с профилями нормальной активности	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
24	IPSec определяет: 1. метод взаимодействия пользователей с VPN 2. наиболее широко признанный, поддерживаемый и стандартизованный из всех протоколов VPN 3. протокол управления содержимым. Почти не используется в VPN	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
25	ESP определяет: 1. безопасно инкапсулированную полезную нагрузку 2. заголовок аутентификации 3. схему обмена ключами через Internet	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
26	Для систем обнаружения вторжений имеются средства анализа: 1. только коммерческие программные средства 2. с открытыми исходными текстами 3. не существует программных средств анализа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
27	Сетевые системы обнаружения вторжений желательно запускать на: 1. одном компьютере с межсетевым экраном 2. одном компьютере с общедоступным сервисом	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01	30

	3. специально выделенном компьютере	ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
28	Размещение сетевой системы обнаружения вторжений в ЛВС позади межсетевого экрана позволяет: 4. прослушивать локальную среду передачи 5. прослушивать среду передачи в демилитаризованной зоне прослушивать среду передачи перед межсетевым экраном	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
29	Безопасность VPN-сетей включает в себя: 1. защиту соединения между хостами в беспроводной локальной сети 2. защиту информации каждого пользователя в сети 3. развертывание информационных услуг посредством функций сети	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
30	Основное достоинство конфигурации "сеть-сеть" состоит в том, что: 1. сети выглядят как смежные, а работа VPN-шлюзов прозрачна для пользователей 2. работа VPN-шлюзов не доступна пользователям 3. полная незащищенность сети	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.1.10. Тестовые вопросы для промежуточной аттестации МДК 02.02

Часть 1

№	Вопрос	ОК/ПК	Время, сек
1	Административные действия в СУБД позволяют выполнять привилегии	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Битовые протоколы передачи данных реализуются на _____ уровне модели взаимодействия открытых систем	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3	Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Как называется процедура предоставления определенному пользователю прав на выполнение некоторых действий?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
5	Что такое IPTV?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	Какое название получила технология, позволяющая обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети с применением средств криптографии?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Восстановление данных является дополнительной функцией услуги защиты	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	Единственный ключ используется в _____ криптосистемах	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Как называют в криптографии сменный элемент шифра, который применяется для шифрования конкретного сообщения	ПК 2.1 ПК 2.2 ПК 2.3	30

		ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
10	Как называется процесс наложения по определенному закону гамма-шифра на открытые данные	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
11	При использовании классических криптографических алгоритмов ключ шифрования и ключ дешифрования совпадают и такие криптосистемы	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
12	Как называется криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись, разработанная в 1977 году	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
13	Маршрутизация и управление потоками данных реализуются на _____ уровне модели взаимодействия открытых систем.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
14	Наиболее надежным механизмом для защиты содержания сообщений является:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
15	Преобразование понятного текста в зашифрованный с целью защиты информации - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03	30

		ОК 04 ОК 09 ОК 10	
16	Слово "криптография" произошло от	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
17	Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
18	Применение услуги причастности рекомендуется на _____ уровне модели OSI	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
19	механизм аутентификации, предполагающий использование определенного устройства для идентификации человеческих характеристик	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
20	устройство контроля доступа в сеть, предназначенное для блокировки всего трафика, за исключением разрешенных данных - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
21	Верно ли утверждение: «поточные шифры применяются для формирования электронной цифровой подписи»?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

22	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
23	Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называется	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
24	Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод …	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
25	Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
26	На сколько блоков будет разбито сообщение размером 1 Кбайт для шифрования алгоритмом DES?Ответ запишите в виде одного числа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
27	Как называется способ шифрования, в котором шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите?	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
28	функция, которая для строки произвольной длины вычисляет некоторое характерное целое значение или некоторую другую строку фиксированной длины	ПК 2.1 ПК 2.2 ПК 2.3	30

		ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
29	Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
30	Наука о скрытой передаче информации путем сохранения в тайне самого факта передачи - это	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

Часть 2

№	Вопрос	ОК/ПК	Время, сек
1	Какие требования предъявляются к корневому каталогу веб-сервера? 1. не должен совпадать с системным корневым каталогом 2. не должен превышать 2 Гбайт 3. должен содержать файл index.html (index.php)	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
2	Межсетевой экран 1. защищает внутренние сети от внешних атак 2. обеспечивает защиту от злоумышленника, использующего для входа в систему законную программу 3. обеспечивает защиту, если злоумышленник через уязвимые места получит доступ к файлам как администратор	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
3	Как называется стандарт для виртуальных локальных сетей? 1. IEEE 802.11 2. IEEE 802.11i 3. IEEE 802.1Q	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
4	Алгоритм DES является	ПК 2.1	30

	1. алгоритмом вычисления функции хеширования 2. алгоритмом формирования электронной цифровой подписи 3. блочным алгоритмом асимметричного шифрования 4. блочным алгоритмом симметричного шифрования	ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
5	Как называется однозначное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины? 1. Хеширование 2. Гаммирование 3. Перестановка	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
6	На чем основана безопасность алгоритма RSA для формирования цифровой подписи? 1. на трудности возведения целых чисел в степень по модулю 2. на трудности вычисления дискретных логарифмов 3. на трудности решения задачи факторизации	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
7	Как называется режим использования блочного шифра, в котором каждый блок исходных данных шифруется независимо от остальных блоков с применением одного и того же ключа шифрования? 1. режим простой поблочной замены 2. режим сцепления блоков шифра 3. режим формирования электронной цифровой подписи 4. режим создания хеш-кода	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
8	192.168.1.1 – это … 1. MAC-адрес 2. SSID 3. IP-адрес в IPv4	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
9	Как называется режим использования блочного шифра, в котором перед шифрованием каждый блок открытого текста складывается по модулю 2 с результатом шифрования предыдущего блока? 1. режим простой поблочной замены 2. режим сцепления блоков шифра 3. режим формирования электронной цифровой подписи	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
10	Алгоритм DES является 1. алгоритмом вычисления функции хеширования 2. алгоритмом формирования электронной цифровой подписи	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01	30

	3. блочным алгоритмом асимметричного шифрования 4. блочным алгоритмом симметричного шифрования	ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
11	Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты? 1. Алгоритм 2. Ключ 3. Протокол 4. Шифр	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
12	Как называется сообщение, полученное после преобразования с использованием любого шифра? 1. закрытым текстом 2. имитовставкой 3. ключом	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
13	Наименее затратный криптоанализ для криптоалгоритма DES 1. перебор по выборочному ключевому пространству 2. разложение числа на сложные множители 3. перебор по всему ключевому пространству 4. разложение числа на простые множители	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
14	Порт 80 позволяет: 1. осуществлять доступ к веб 2. передавать файлы 3. получать и отсылать почту	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
15	Что является основной причиной распространения использования беспроводных технологий? 1. недорогой метод соединения информационных систем 2. высокая скорость передачи данных 3. высокая защищенность соединений	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
16	Что в криптографии называют открытым текстом? 1. исходное сообщение (сообщение до шифрования) 2. открытый ключ шифрования 3. сообщение, получение после преобразования с использованием любого шифра 4. электронную цифровую подпись	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК	30

		09 ОК 10	
17	В чем суть метода открытого и скрытого ключей? 1. криптование скрытым ключом и декриптование открытым ключом; 2. использование суммы двух ключей в качестве ключа для криптования; 3. криптование открытым ключом и декриптование скрытым ключом.	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
18	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства? 1. шифр Маркова 2. шифр Цезаря 3. шифр Энигма 4. шифр Бэбиджа	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
19	Какая наука разрабатывает методы «вскрытия» шифров? 1. Криптография 2. Криптоанализ 3. Тайнопись	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
20	Что такое криптостойкость? 1. характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа 2. свойство гаммы 3. все ответы верны	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
21	Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности? 1. алгоритмом гаммирования 2. алгоритмом перестановки 3. алгоритмом аналитических преобразований	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
22	Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера: 1. 4 2. 3 3. 5	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
23	Суть метода перестановки:	ПК 2.1	30

	1. символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов 2. замена алфавита 3. все правильные	ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
24	К основным функциям системы безопасности можно отнести все перечисленное: 1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
25	Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: 1. Регламентированной 2. Правовой 3. Защищаемой	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
26	Риски в сфере информационной безопасности разделяются на: 1. внешние и внутренние 2. объективные и субъективные 3. системные и операционные	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
27	При полномочной политике безопасности совокупность меток с одинаковыми значениями образует: 1. область равного доступа; 2. уровень безопасности 3. уровень доступности	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
28	Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты? 1. Алгоритм 2. Ключ 3. Протокол 4. Шифр	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30
29	Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется:	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01	30

	1. актуальностью информации 2. доступностью 3. качеством информации 4. целостностью	ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	
30	Согласно «Оранжевой книге» уникальные идентификаторы должны иметь: 1. наиболее важные субъекты 2. наиболее важные объекты 3. все субъекты 4. все объекты	ПК 2.1 ПК 2.2 ПК 2.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 09 ОК 10	30

3.2. 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 ранееизученным материалом из курса дисциплины, а также с материалом, усвоенным при изучении других дисциплин/модулей. **Оценка «4»** ставится, если ответ обучающегося удовлетворяет основным 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 основнымизнаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для оценки.

2	Тесты	**«5»** - 100 – 91% правильных ответов **«4»** - 90 - 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	**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.
5	Лабораторные работы	**Оценка «5»** ставится, если студент демонстрирует знание теоретического и практического материала по теме лабораторной работы, определяет взаимосвязи между показателями условий, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. **Оценка «4»** ставится, если студент демонстрирует знание теоретического и практического материала по теме лабораторной работы, допуская незначительные неточности при решении задания, имея неполное понимание междисциплинарных связей при правильном выборе алгоритма решения задания. **Оценка «3»** ставится, если студент затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, требующий наводящих вопросов преподавателя, выбор алгоритма решения задачи возможен при наводящих вопросах преподавателя. **Оценка «2»** ставится, если студент дает неверную оценку ситуации, неправильно выбирает алгоритм действий.
6	Самостоятельная работа	**Оценка «5»** ставится, если обучающийся демонстрирует знание изученного материала по теме самостоятельной работы, определяет взаимосвязи между показателями задачи, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. **Оценка «4»** ставится, если обучающийся демонстрирует знание изученного материала по теме самостоятельной работы, допуская незначительные неточности при решении задач, имея неполное понимание междисциплинарных связей при правильном выборе алгоритма решения задания. **Оценка «3»** ставится, если обучающийся затрудняется с правильным решением предложенного задания, дает неполный ответ, требующий наводящих вопросов преподавателя, выбор алгоритма решения задания возможен при наводящих вопросах преподавателя. **Оценка «2»** ставится, если обучающийся не выполнил предложенное задание.

3.3. Фонд оценочных средств для промежуточной аттестации по ПМ 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

I. ПАСПОРТ

Назначение:

Фонд оценочных средств предназначен для контроля и оценки результатов освоения ПМ. 02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе криптографических средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

II. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

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

Рассмотрено на заседании предметной (цикловой) комиссии _____2022г. Председатель _____Н.В. Кривоносова	***Экзаменационный билет* № Н** По профессиональному модулю ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе криптографических средств защиты Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем	УТВЕРЖДАЮ Заместитель директора по учебной работе колледжа _____Н.В. Калинина 2022г.

Инструкция для обучающихся Внимательно прочитайте задание.

Время выполнения задания – 120 минут

Задание 1. Выполните настройку программных и программно-аппаратных средств защиты информации для обеспечения защиты информации в информационно-телекоммуникационных системах и сетях

Задание 2. Выполните настройку криптографических средств защиты информации для обеспечения защиты информации в информационно-телекоммуникационных системах и сетях

*Преподаватель*_____И.О. Фамилия

III. ПАКЕТ ЭКЗАМЕНАТОРА

III а. УСЛОВИЯ

Время выполнения задания – 120 минут

Оборудование:

- посадочные места с ПК по количеству обучающихся;
- рабочее место преподавателя;
- калькуляторы.

Работа обучающегося оценивается путем устного ответа с демонстрацией и пояснением выполненной работы. Длительность ответа – не более 10 минут.

Задания к экзамену по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе криптографических средств защиты

Задание 1. Выполните настройку программных и программно-аппаратных средств защиты информации для обеспечения защиты информации в информационно-телекоммуникационных системах и сетях

1. Задача по настройке безопасности ОС Windows:
- Шаг 1: Установить ОС Windows на виртуальную машину.
- Шаг 2: Настроить политику паролей и блокировку экрана.
- Шаг 3: Настроить антивирусную программу и запланировать ежедневную проверку системы.
- Шаг 4: Настроить межсетевой экран и открыть только необходимые порты.
- Шаг 5: Настроить обновления ОС и приложений для устранения уязвимостей.
- Шаг 6: Запланировать резервное копирование данных.

2. Разработка модели безопасности на основе мандатной политики:
- Шаг 1: Определить уровни доступа пользователей и объектов в системе.
- Шаг 2: Создать таблицу доступа, определяющую права доступа пользователей к объектам системы.
- Шаг 3: Настроить политику безопасности на основе созданной таблицы.
- Шаг 4: Создать пользователя и проверить права доступа.

3. Разработка модели безопасности на основе ролевой политики:
- Шаг 1: Определить роли пользователей и объекты, к которым они имеют доступ.
- Шаг 2: Создать таблицу ролей, определяющую связь между ролями и объектами системы.
- Шаг 3: Настроить политику безопасности на основе созданной таблицы.
- Шаг 4: Создать пользователя и назначить ему роль.

4. Резервирование данных:
- Шаг 1: Определить данные, которые требуется резервировать.
- Шаг 2: Выбрать программное обеспечение для резервного копирования.
- Шаг 3: Настроить расписание резервного копирования.
- Шаг 4: Проверить корректность резервного копирования.

5. Разграничение доступа в ОС Windows:
- Шаг 1: Создать группы пользователей и назначить им права доступа.
- Шаг 2: Создать пользователей и назначить их в нужные группы.
- Шаг 3: Настроить права доступа к файлам и папкам.
- Шаг 4: Проверить корректность настроек.

6. Настройка межсетевого экрана:
- Шаг 1: Определить правила доступа к сети.
- Шаг 2: Настроить правила фильтрации пакетов и доступа к определенным портам. Шаг 3:

Настроить список исключений. Шаг 4: Проверить работоспособность межсетевого экрана.

7. Настройка VPN:
- Шаг 1: Установить и настроить VPN-сервер.
- Шаг 2: Создать профили пользователей и назначить им права доступа.
- Шаг 3: Настроить шифрование трафика и сертификаты безопасности.
- Шаг 4: Проверить работу VPN-соединения.

8. Настройка системы обнаружения вторжений:
- Шаг 1: Установить и настроить систему обнаружения вторжений (IDS/IPS).
- Шаг 2: Создать правила обнаружения вторжений и исключения.
- Шаг 3: Настроить оповещение о возможных атаках.
- Шаг 4: Проверить работу системы обнаружения вторжений.

9. Организация защиты компьютерной системы:
- Шаг 1: Оценить уязвимости компьютерной системы.
- Шаг 2: Установить и настроить необходимое программное и аппаратное обеспечение.
- Шаг 3: Разработать стратегию бэкапирования и резервного копирования данных.
- Шаг 4: Провести тестирование на проникновение.

10. Настройка отделов и групповых политик в DLP-системе Search Inform:
- Шаг 1: Создать группы пользователей и отделов.
- Шаг 2: Настроить правила обнаружения и контроля передачи конфиденциальных данных.
- Шаг 3: Настроить мониторинг и оповещение о нарушениях безопасности.
- Шаг 4: Проверить работоспособность системы DLP.

11. Настройка системы обнаружения вторжений:
- Шаг 1: Установить программу системы обнаружения вторжений (например, Snort).
- Шаг 2: Создать файл конфигурации программы.
- Шаг 3: Настроить правила обнаружения вторжений.
- Шаг 4: Проверить работу программы на тестовой среде.

12. Организация защиты компьютерной системы:
- Шаг 1: Оценить уязвимости системы.
- Шаг 2: Установить антивирусное программное обеспечение.
- Шаг 3: Настроить правила межсетевого экрана.
- Шаг 4: Настроить систему обнаружения вторжений.
- Шаг 5: Настроить резервное копирование данных.
- Шаг 6: Провести обучение пользователей вопросам информационной безопасности.

13. Настройка отделов и групповых политик в DLP-системе Search Inform:
- Шаг 1: Установить программу DLP-системы Search Inform.
- Шаг 2: Создать отделы и группы пользователей.
- Шаг 3: Настроить права доступа для каждой группы пользователей.
- Шаг 4: Настроить правила мониторинга и блокировки данных в соответствии с требованиями компании.
- Шаг 5: Проверить работу системы на тестовых данных.

14. Настройка безопасности Wi-Fi-сети:
- Шаг 1: Определить тип шифрования и установить его.
- Шаг 2: Настроить пароль доступа к сети.
- Шаг 3: Ограничить доступ к сети по MAC-адресам устройств.
- Шаг 4: Проверить корректность настроек.

15. Разработка политики удаленного доступа к серверам:
- Шаг 1: Определить список пользователей и их права доступа.
- Шаг 2: Настроить удаленный доступ по протоколу SSH.
- Шаг 3: Ограничить доступ по IP-адресам.
- Шаг 4: Проверить корректность настроек.

16. Настройка системы антивирусной защиты:

- Шаг 1: Установить антивирусное ПО на компьютер.
- Шаг 2: Настроить автоматические проверки файлов и директорий.
- Шаг 3: Настроить автоматические обновления антивирусной базы данных.
- Шаг 4: Проверить корректность настроек.

17. Разработка механизма резервного копирования данных:
- Шаг 1: Определить список файлов и директорий для резервного копирования.
- Шаг 2: Выбрать метод резервного копирования (полный, инкрементальный, дифференциальный).
- Шаг 3: Настроить расписание резервного копирования.
- Шаг 4: Проверить корректность настроек.

18. Настройка механизма шифрования файлов:
- Шаг 1: Установить ПО для шифрования файлов.
- Шаг 2: Создать ключ шифрования.
- Шаг 3: Настроить права доступа к зашифрованным файлам.
- Шаг 4: Проверить корректность настроек.

19. Разработка политики безопасности сетевых служб:
- Шаг 1: Определить список сетевых служб, доступных для использования.
- Шаг 2: Определить список пользователей и их права доступа к сетевым службам.
- Шаг 3: Ограничить доступ к сетевым службам по IP-адресам.
- Шаг 4: Проверить корректность настроек.

20. Настройка протоколирования событий в ОС Windows:
- Шаг 1: Открыть центр управления безопасностью.
- Шаг 2: Выбрать опцию "Аудит событий".
- Шаг 3: Настроить параметры протоколирования событий в соответствии с требованиями безопасности.
- Шаг 4: Проверить правильность настроек.

21. Настройка системы контроля целостности файлов:
- Шаг 1: Установить программу контроля целостности файлов, например, Tripwire.
- Шаг 2: Создать базу данных для хранения информации о контролируемых файлах.
- Шаг 3: Настроить систему для контроля целостности файлов.
- Шаг 4: Проверить работу системы контроля целостности файлов.

22. Разработка и настройка системы шифрования данных:
- Шаг 1: Выбрать программное обеспечение для шифрования данных, например, VeraCrypt.
- Шаг 2: Установить и настроить программу шифрования.
- Шаг 3: Создать зашифрованный том для хранения данных.
- Шаг 4: Проверить правильность настроек системы шифрования.

23. Настройка системы контроля доступа к сетевым ресурсам:
- Шаг 1: Выбрать программное обеспечение для контроля доступа к сетевым ресурсам, например, Access Manager.
- Шаг 2: Установить и настроить программу контроля доступа к сетевым ресурсам.
- Шаг 3: Создать правила доступа для пользователей и групп пользователей.
- Шаг 4: Проверить работу системы контроля доступа к сетевым ресурсам.

24. Разработка и настройка системы мониторинга безопасности:
- Шаг 1: Выбрать программное обеспечение для мониторинга безопасности, например, Security Center.
- Шаг 2: Установить и настроить программу мониторинга безопасности.
- Шаг 3: Создать правила мониторинга для обнаружения угроз безопасности.
- Шаг 4: Проверить работу системы мониторинга безопасности.

25. Настройка биометрической аутентификации в ОС Windows 10:
- Шаг 1: Проверить поддерживается ли ваше устройство считывания биометрических данных в Windows 10.
- Шаг 2: Настроить устройство считывания в драйверах Windows.

- Шаг 3: Настроить параметры аутентификации через биометрию.
- Шаг 4: Проверить работоспособность аутентификации через биометрию.

Задание 2. Выполните настройку криптографических средств защиты информации для обеспечения защиты информации в информационно-телекоммуникационных системах и сетях

1. Установите VipNet/SecretNet на сервер и настройте его для работы в вашей сети.
2. Настройте аутентификацию пользователей VipNet/SecretNet через Active Directory.
3. Создайте политики безопасности для VipNet/SecretNet, чтобы ограничить доступ к ресурсам сети только для авторизованных пользователей.
4. Настройте шифрование данных для всех трафика, проходящего через VipNet/SecretNet.
5. Настройте VipNet/SecretNet для работы в режиме "туннельного" шифрования, чтобы защитить данные, передаваемые через открытые сети, такие как Интернет.
6. Настройте фильтрацию трафика, чтобы блокировать попытки неавторизованного доступа к сети.
7. Настройте мониторинг и журналирование для VipNet/SecretNet, чтобы отслеживать любые попытки нарушения безопасности.
8. Настройте систему уведомлений, чтобы быстро реагировать на любые попытки нарушения безопасности.
9. Создайте профили пользователей для управления доступом к ресурсам в вашей сети.
10. Настройте группы пользователей для легкого управления доступом к ресурсам.
11. Настройте политики паролей для VipNet/SecretNet, чтобы гарантировать, что все пароли сложны и изменяются регулярно.
12. Настройте функцию блокировки пользователей, чтобы предотвратить неудачные попытки аутентификации.
13. Создайте отчеты об активности пользователей, чтобы отслеживать любые подозрительные действия.
14. Настройте механизмы защиты от DDoS-атак для VipNet/SecretNet.
15. Настройте механизмы защиты от ARP-атак для VipNet/SecretNet.
16. Настройте механизмы защиты от IP-атак для VipNet/SecretNet.
17. Настройте функцию восстановления после сбоя, чтобы быстро вернуть VipNet/SecretNet к работе в случае сбоя или отказа.
18. Настройте функцию резервирования, чтобы обеспечить непрерывную работу VipNet/SecretNet в случае отказа оборудования.
19. Настройте VipNet/SecretNet для работы с другими средствами защиты информации, такими как антивирусное программное обеспечение или межсетевой экран.
20. Настройте VipNet/SecretNet для работы в виртуальной среде.
21. Настройте VipNet/SecretNet для работы с различными операционными системами, такими как Windows, Linux, macOS и т.д.
22. Создайте и настройте VPN-туннели для удаленных пользователей, чтобы обеспечить безопасный доступ к ресурсам сети из любой точки мира.
23. Настройте механизмы проверки целостности данных, чтобы обнаруживать и предотвращать любые попытки изменения или подмены данных.
24. Настройте VipNet/SecretNet для работы в различных режимах шифрования, например, AES, DES, RSA и т.д., в зависимости от потребностей вашей сети.

25. Настройте VipNet/SecretNet для автоматического обновления и обновления безопасности, чтобы гарантировать, что ваша сеть всегда защищена от новых угроз и уязвимостей.

III б. 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, схему, модель, программу 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-схем, графиков

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	

4. ЛИСТ СОГЛАСОВАНИЯ

Дополнения и изменения к комплекту КОС

Дополнения и изменения к комплекту КОС на_____учебный год по профессиональному модулю _____

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