

Министерство науки и высшего образования Российской Федерации
 федеральное государственное бюджетное образовательное учреждение высшего образования
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
 ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»**

УТВЕРЖДАЮ
 Первый проректор, проректор по учебной
 работе

_____ А.Е. Рудин
 «30 » 06 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.20 <small>(Индекс дисциплины)</small>	Программно-аппаратные средства защиты информации <small>(Наименование дисциплины)</small>
Кафедра: 20 <small>Код</small>	Интеллектуальных систем и защиты информации <small>Наименование кафедры</small>
Направление подготовки: 10.03.01 Информационная безопасность	Безопасность компьютерных систем (в коммерческих структурах)
Профиль подготовки:	
Уровень образования: бакалавриат	

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	180		
	Аудиторные занятия	68		
	Лекции	34		
	Лабораторные занятия	17		
	Практические занятия	17		
	Самостоятельная работа	85		
	Промежуточная аттестация	27		
Формы контроля по семестрам (номер семестра)	Экзамен	5		
	Зачет			
	Контрольная работа			
	Курсовой проект (работа)	5		
Общая трудоемкость дисциплины (зачетные единицы)		5		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная					5							
Очно-заочная												
Заочная												

Программа государственной итоговой аттестации составлена в соответствии с федеральным
государственным образовательным стандартом высшего образования
по соответствующему направлению подготовки

и на основании учебного плана № 1/1/704

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1: Базовая Обязательная Дополнительно является факультативом
 Вариативная По выбору

1.2. Цель дисциплины

Сформировать компетенции обучающегося в области программно-аппаратных средств защиты информации.

1.3. Задачи дисциплины

- Рассмотреть классификацию и область применения программно-аппаратных средств защиты информации
- Рассмотреть криптографические основы защиты информации
- Рассмотреть методы и средства аутентификации и разграничения доступа
- Рассмотреть методы и средства защиты информации в корпоративных сетях
- Рассмотреть средства организации комплексной защиты информации

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Второй
Планируемые результаты обучения Знать: состав и классификацию защищаемой информации с помощью программно-аппаратных средств Уметь: устанавливать влияние факторов на достоверность полученной информации Владеть: методами и средствами выявления угроз безопасности автоматизированным системам		
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Второй
Планируемые результаты обучения Знать: места уязвимости программного обеспечения и программно-аппаратных средств защиты Уметь: определять направления использования аппаратного и программного обеспечения определенного класса для решения служебных задач Владеть: навыками выявления и уничтожения компьютерных вирусов		
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Второй
Планируемые результаты обучения Знать: принципы построения программно-аппаратных средств защиты информации Уметь: применять современные программно-аппаратные системы защиты информации		

Код компетенции	Формулировка компетенции	Этап формирования
Владеть: Навыками организации защиты данных при сетевом взаимодействии		
ПСК-1	Готовность к администрированию программно-аппаратных средств защиты информации в компьютерных сетях	Первый
Планируемые результаты обучения Знать: Понятия идентификации и аутентификации Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Владеть: средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

- Основы информационной безопасности (ПК-7)
- Безопасность жизнедеятельности (ПСК-1)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Введение			
Тема 1. Обзор программно-аппаратных средств защиты информации	8		
Тема 2. Криптографическая защита информации	8		
Текущий контроль 1 (опрос)	1		
Учебный модуль 2. Управление доступом			
Тема 3. Идентификация, аутентификация и управление доступом	8		
Тема 4. Доверенная загрузка ПК	8		
Тема 5. СКУД	8		
Текущий контроль 2 (опрос)	1		
Учебный модуль 3. Защита корпоративных сетей			
Тема 6. Протоколы защищенных каналов	8		
Тема 7. Межсетевое экранирование	7		
Тема 8. Технологии виртуальных защищенных сетей VPN	8		
Тема 9. Защита удаленного доступа	8		
Тема 10. Технологии обнаружения и предотвращения вторжений	8		
Тема 11. Технологии защиты от вредоносных программ и спама	8		
Текущий контроль 3 (опрос)	1		
Учебный модуль 4. Средства управления информационной безопасностью			
Тема 12. Системы предотвращения утечек данных (DLP)	8		
Тема 13. Управление информацией и событиями ИБ (SIEM)	8		
Тема 14. Threat Intelligence	8		
Тема 15. Security Operation Center (SOC)	8		
Текущий контроль 4 (опрос)	1		
Курсовая работа (проект)	30		
Промежуточная аттестация по дисциплине (Экзамен)	27		
ВСЕГО:	180		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	5	2				
2	5	2				
3	5	4				
4	5	2				
5	5	2				
6	5	2				
7	5	2				
8	5	2				
9	5	2				
10	5	2				
11	5	2				
12	5	2				
13	5	2				
14	5	2				
15	5	4				
ВСЕГО:		34				

3.2. Практические и семинарские занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Службы и документы информационной безопасности (практическое занятие)	5	1				
2	Рассмотрение примеров криптографических механизмов (практическое занятие)	5	1				
3	Работа с криптографическими картами (практическое занятие)	5	2				
4	Принципы работы модуля доверенной загрузки (практическое занятие)	5	1				
5	Проектирование СКУД (практическое занятие)	5	1				
6	Рассмотрение средств защиты сетевых каналов (практическое занятие)	5	1				
7	Рассмотрение технологий и средств межсетевого экранирования (практическое занятие)	5	1				
8	Рассмотрение технологий виртуальных защищенных сетей VPN (практическое занятие)	5	1				
9	Рассмотрение технологий защиты удаленного доступа (практическое занятие)	5	1				
10	Рассмотрение технологий обнаружения и предотвращения вторжений (практическое занятие)	5	1				

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
11	Рассмотрение технологий защиты от вредоносных программ и спама (практическое занятие)	5	1				
12	Рассмотрение систем предотвращения утечек данных (практическое занятие)	5	1				
13	Рассмотрение систем SIEM (практическое занятие)	5	1				
14	Рассмотрение технологий Threat Intelligence (практическое занятие)	5	1				
15	Организация SOC (практическое занятие)	5	2				
ВСЕГО:			17				

3.3. Лабораторные занятия

Номера изучаемых тем	Наименование лабораторных занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
2	Исследование GPG	5	2				
3	Исследование смарт-карт	5	2				
4	Исследование комплекса «АККОРД»	5	2				
7	Исследование средств Cisco МЭ	5	2				
8	Исследование средств Cisco VPN	5	2				
10	Исследование Snort	5	2				
12	Исследование MyDLP	5	2				
13	Исследование OSSIM	5	3				
ВСЕГО:			17				

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

4.1. Цели и задачи курсовой работы (проекта)

Целью курсовой работы является исследование современного состояния российского рынка программно-аппаратных средств защиты информации.

Задачи:

- изучить теоретические основы функционирования исследуемых типов средств;
- проанализировать современное состояние рынка исследуемых средств.

4.2. Тематика курсовой работы (проекта)

- 1) сформировать теоретические основы функционирования исследуемых типов средств;
- 2) составить перечень продуктов, предлагаемых на российском рынке;
- 3) провести категоризацию средств по области применения;
- 4) провести сравнительный анализ стоимости и функциональных и нагрузочных характеристик внутри каждой категории.

4.3. Требования к выполнению и представлению результатов курсовой работы

Работа выполняется индивидуально, с использованием данных из сети Интернет.

Результаты представляются в виде отчета объемом не менее 40 страниц, содержащего следующие обязательные элементы:

- титульный лист;
- оглавление;
- введение;
- теоретические основы функционирования СЗИ;
- средства защиты, представленные на рынке;
- сравнительный анализ средств;
- заключение;

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1-4	Опрос	5	4				

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	5	30				
Подготовка к практическим (семинарским) и лабораторным занятиям	5	25				
Выполнение курсовых работ	5	30				
Подготовка к экзаменам	5	27				
ВСЕГО:		112				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Лекции	<i>Лекция-беседа</i>	10		
Практические и семинарские занятия	<i>Занятия в группах, анализ проблемных ситуаций</i>	10		
Лабораторные занятия	<i>Занятия в группах</i>	10		
ВСЕГО:		30		

7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

Перечень и параметры оценивания видов деятельности обучающегося

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов

1	Аудиторная активность: посещение лекций и практических (семинарских) занятий	5	17 лекций и 17 практических занятий, по 2,5 балла за каждое занятие, максимум 85 баллов 15 баллов за выполнение реферата на практическом занятии
2	Текущий контроль	15	4 опроса по 5 вопросов в каждом, за каждый вопрос максимум по 5 баллов. максимум 100 баллов
3	Выполнение лабораторных работ	10	13 лабораторных работ, по 8 баллов за успешную сдачу каждой работы, максимум 100 баллов. 4 балла за защиту работы можно получить при полном и правильном выполнении задания, предоставлении отчета с корректным оформлением и правильных ответах на вопросы по лабораторной. За недочеты и ошибки баллы снижаются
4	Сдача курсовой работы	30	100 баллов за защиту курсовой работы ставится, если обучающийся: <ul style="list-style-type: none"> • предоставил правильно оформленный отчет; • защитил работу в срок; • выполнил работу в полном объеме; • не допустил ошибок в работе; • правильно и исчерпывающе ответил на вопросы преподавателя на тему работы. За нарушения условий в списке баллы снижаются пропорционально тяжести нарушения.
5	Сдача зачета	40	Ответы на теоретические вопросы (полнота, владение терминологией, затраченное время) – максимум 30 баллов за каждый вопрос (всего 2 вопроса); Решение практической задачи – до 40 баллов.
Итого (%):		100	

Перевод балльной шкалы в традиционную систему оценивания

Баллы	Оценка по нормативной шкале	
86 - 100	5 (отлично)	Зачтено
75 – 85	4 (хорошо)	
61 – 74		
51 - 60	3 (удовлетворительно)	
40 – 50		
17 – 39	2 (неудовлетворительно)	Не зачтено
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: <http://www.iprbookshop.ru/63594.html>.— ЭБС «IPRbooks»
1. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс]: учебное пособие/ В.И. Петренко— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 201 с.— Режим доступа: <http://www.iprbookshop.ru/66023.html>.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Бисюков В.М. Защита и обработка конфиденциальных документов [Электронный ресурс]: практикум/ В.М. Бисюков— Электрон. текстовые данные.— Ставрополь: Северо-Кавказский

федеральный университет, 2016.— 116 с.— Режим доступа:

<http://www.iprbookshop.ru/66060.html>.— ЭБС «IPRbooks»

2. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]:

лабораторный практикум/ И.А. Калмыков, Д.О. Науменко, Т.А. Гиш— Электрон. текстовые

данные.— Ставрополь: Северо-Кавказский федеральный университет, 2015.— 109 с.— Режим

доступа: <http://www.iprbookshop.ru/63099.html>.— ЭБС «IPRbooks»

3. Методы и средства обеспечения программно-аппаратной защиты информации [Электронный

ресурс]: научно-техническое издание/ А.И. Астайкин [и др.].— Электрон. текстовые данные.—

Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015.— 224 с.— Режим доступа:

<http://www.iprbookshop.ru/60959.html>.— ЭБС «IPRbooks»

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Спицкий, С. В. Эффективная аудиторная и самостоятельная работа обучающихся:

методические указания / С. В. Спицкий. – СПб.: СПбГУПТД, 2015. – Режим доступа:

http://publish.sutd.ru/tp_get_file.php?id=2015811, по паролю.

2. Караулова, И. Б. Организация самостоятельной работы обучающихся / И. Б. Караулова, Г. И.

Мелешкова, Г. А. Новоселов. – СПб.: СПГУТД, 2014. – 26 с. – Режим доступа

http://publish.sutd.ru/tp_get_file.php?id=2014550, по паролю.

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. The GNU Privacy Guard [Электронный ресурс]. – Режим доступа:

<https://www.gnupg.org/index.html>

2. Семейство ПАК СЗИ НСД Аккорд [Электронный ресурс]. – Режим доступа: <http://www.accord.ru>

3. Navigating the Cisco ASA Series Documentation [Электронный ресурс]. – Режим доступа:

<https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html>

4. Snort - Network Intrusion Detection & Prevention System [Электронный ресурс]. – Режим доступа:

<https://www.snort.org>

5. Data Loss Prevention Solutions [Электронный ресурс]. – Режим доступа: <https://www.mydlp.com>

6. AlienVault OSSIM [Электронный ресурс]. – Режим доступа:

<https://www.alienvault.com/products/ossim>

7. Электронно-библиотечная система IPRbooks. (<http://www.iprbookshop.ru>)

8. Электронная библиотека учебных изданий СПбГУПТД (<http://publish.sutd.ru>)

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. VirtualBox

2. GPG

3. GNS3

4. Snort

5. MyDLP

6. OSSIM

7. Microsoft Office Standart 2016 Russian Open No Level Academic)

8. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) +

Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level

Academic

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. Компьютерный класс с возможностью выхода в Интернет

2. Проектор

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	Лекции обеспечивают теоретическое изучение дисциплины. На лекциях излагается основное содержание курса, иллюстрируемое конкретными примерами, широко используется зарубежный и отечественный опыт по соответствующей тематике.

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
	<p>Освоение лекционного материала обучающимся предполагает следующие виды работ:</p> <ul style="list-style-type: none"> • проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины; • конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины. <p>Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии</p>
Практические занятия	На практических занятиях (семинарах) разъясняются теоретические положения курса, обучающиеся работают с конкретными ситуациями, овладевают навыками сбора, анализа и обработки информации для принятия самостоятельных решений, навыками подготовки информационных обзоров и аналитических отчетов по соответствующей тематике.
Лабораторные занятия	В процессе выполнения лабораторных работ обучающийся учится применять положения теоретического курса при реализации программного обеспечения. Следует предварительно изучить методические указания по выполнению лабораторных работ.
Самостоятельная работа	<p>Данный вид работы предполагает расширение и закрепление знаний, умений и навыков, усвоенных на аудиторных занятиях путем самостоятельной проработки учебно-методических материалов по дисциплине и другим источникам информации; выполнения рефератов; подготовку к экзамену. Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством (при участии) преподавателя.</p> <p>При подготовке к экзамену необходимо ознакомиться с демонстрационным вариантом задания (перечнем вопросов), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя.</p>

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ПК-1	<p>Приводит примеры программных и аппаратных продуктов для обеспечения защиты информации</p> <p>Систематизирует основные угрозы, связанные с нарушением целостности и достоверности передаваемой информации</p> <p>Проводит установку основных программно-аппаратных средств для обеспечения эффективной защиты информации</p>	<p>Вопросы для устного собеседования</p> <p>Практическое задание</p>	<p>Вопросы (4)</p> <p>Задания (10)</p>
ПК-6	<p>Формулирует направления, методы и средства защиты информации от утечки, хищения, искажения, подделки, несанкционированного уничтожения, копирования и блокирования</p> <p>выбирает, строит и анализирует показатели защищенности программно-аппаратных средств защиты информации</p> <p>настраивает средства обнаружения вторжений и антивирусные системы</p>	<p>Вопросы для устного собеседования</p> <p>Практическое задание</p>	<p>Вопросы (5)</p> <p>Задания (10)</p>
ПК-7	Объясняет механизмы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием программных и аппаратных комплексов	Вопросы для устного собеседования	Вопросы (18)

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
	Составляет перечень инструментария, обеспечивающего программно-аппаратную защиту информационных ресурсов от модификации Предлагает меры обеспечения безопасной работы в сети	Практическое задание	Задания (10)
ПСК-1	Описывает назначение и принципы действия систем идентификации и аутентификации объектов и субъектов ИТ Выстраивает комплексную систему защиты информации по принципу разумной достаточности с применением современных программно-аппаратных средств Составляет обоснованный план защиты рабочих мест с использованием современных программно-аппаратных средств информационной безопасности	Вопросы для устного собеседования Практическое задание	Вопросы (9) Задания (10)

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Баллы	Оценка по традиционной шкале	Критерии оценивания сформированности компетенций	
		Устное собеседование	Курсовая работа
86 - 100	5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу. Учитываются баллы, накопленные в течение семестра.	Критическое и разностороннее рассмотрение вопросов, свидетельствующее о значительной самостоятельной работе с источниками. Качество исполнения всех элементов задания полностью соответствует всем требованиям. Учитываются баллы, накопленные в течение семестра.
75 – 85	4 (хорошо)	Ответ полный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный. Учитываются баллы, накопленные в течение семестра.	Все заданные вопросы освещены в необходимой полноте и с требуемым качеством. Ошибки отсутствуют. Самостоятельная работа проведена в достаточном объеме, но ограничивается только основными рекомендованными источниками информации. Учитываются баллы, накопленные в течение семестра.
61 – 74		Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки. Учитываются баллы, накопленные в течение семестра.	Работа выполнена в соответствии с заданием. Имеются отдельные несущественные ошибки или отступления от правил оформления работы. Учитываются баллы, накопленные в течение семестра.
51 - 60	3 (удовлетворительно)	Ответ воспроизводит в основном только лекционные материалы, без самостоятельной работы с рекомендованной литературой. Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам. Учитываются баллы, накопленные	Задание выполнено полностью, но в работе есть отдельные существенные ошибки, либо качество представления работы низкое, либо работа представлена с опозданием. Учитываются баллы, накопленные в течение семестра.

		в течение семестра.	
40 – 50		Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов. Учитываются баллы, накопленные в течение семестра.	Задание выполнено полностью, но с многочисленными существенными ошибками. При этом нарушены правила оформления или сроки представления работы. Учитываются баллы, накопленные в течение семестра.
17 – 39	2 (неудовлетворительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Не учитываются баллы, накопленные в течение семестра.	Отсутствие одного или нескольких обязательных элементов задания, либо многочисленные грубые ошибки в работе, либо грубое нарушение правил оформления или сроков представления работы. Не учитываются баллы, накопленные в течение семестра.
1 – 16		Непонимание заданного вопроса. Неспособность сформулировать хотя бы отдельные концепции дисциплины. Не учитываются баллы, накопленные в течение семестра.	Содержание работы полностью не соответствует заданию. Не учитываются баллы, накопленные в течение семестра.
0		Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки). Не учитываются баллы, накопленные в течение семестра.	Представление чужой работы, плагиат, либо отказ от представления работы. Не учитываются баллы, накопленные в течение семестра.

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Классификация программно-аппаратных средств защиты информации	1
2	Классификация рисков, которые можно снизить применением программно-аппаратных средств защиты информации	1
3	Основные криптографические механизмы	2
4	Сертификаты и PKI	2
5	Методы простой аутентификации	2
6	Методы аппаратной аутентификации	3
7	Криптографические протоколы аутентификации	3
8	Биометрическая аутентификация	3
9	Принципы AAA и SSO	3
10	Принципы работы модулей доверенной загрузки	4
11	Поддержка операций по обеспечению безопасности аппаратными модулями создания доверенной среды	4
12	Состав и назначение СКУД	5
13	Принципы организации и проектирования систем СКУД	5
14	Протоколы PPTP и L2TP	6
15	Протокол IPSec	6
16	Протокол SSL (TLS)	6
17	Протокол SOCKS	6
18	Принципы межсетевого экранирования	7
19	Типовые схемы организации межсетевого экранирования	7
20	Принципы VPN	8
21	Основные схемы организации VPN	8
22	Принципы организации удаленного доступа	9
23	Основные схемы удаленного доступа	9
24	Принципы технологии обнаружения и предотвращения вторжений	10
25	Основные схемы организации обнаружения и предотвращения вторжений	10
26	Принципы защиты от вредоносных программ и спама	11
27	Основные схемы организации защиты от вредоносных программ	11

28	Принципы технологии предотвращения утечек данных	12
29	Типовые схемы организации защиты от утечек данных	12
30	Принципы управления событиями (SIEM)	13
31	Принципы управления информацией (SIEM)	13
32	Основные схемы внедрения SIEM	13
33	Основные процессы Threat Intelligence	14
34	Основные методы оценки эффективности Threat Intelligence	14
35	Развитие и принципы SOC, этапы построения	15
36	Используемые технологии для организации SOC	15

Вариант типовых заданий (задач, кейсов), разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия типовых задач (задач, кейсов)	Ответ
1	Сформировать команды для создания списка контроля доступа для маршрутизатора Cisco: блокировать все пакеты, кроме идущих от всех источников по протоколу TCP на хост 10.0.20.159 на порты 443 и 80	ip access-list extended test permit tcp any host 10.0.20.159 eq 80 permit tcp any host 10.0.20.159 eq 443 deny any any
2	Сформировать команды для создания списка контроля доступа для маршрутизатора Cisco: блокировать все пакеты, кроме идущих из сетей 10.45.0.0/16 и 10.50.0.0/16 на диапазон портов 0 – 1024 по протоколу TCP. Разрешить все ICMP пакеты.	ip access-list extended test permit tcp 10.45.0.0 0.0.255.255 any lt 1024 permit tcp 10.50.0.0 0.0.255.255 any lt 1024 permit icmp any any deny any any
3	Сформировать команды для создания списка контроля доступа для маршрутизатора Cisco: разрешить все пакеты, кроме идущих от всех источников по протоколу TCP на хост 10.0.20.159 на порты 443 и 80	ip access-list extended test deny tcp any host 10.0.20.159 eq 80 deny tcp any host 10.0.20.159 eq 443 permit any any

10.3. Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче (экзамена, зачета и / или защите курсовой работы) и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная письменная компьютерное тестирование иная*

*В случае указания формы «Иная» требуется дать подробное пояснение

10.3.3. Особенности проведения экзамена

Обучающийся тянет билет, в котором два теоретических вопроса и задача. После этого готовится в течении как минимум 15 минут с использованием конспекта лекций и других материалов. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. Отвечает на сопутствующие вопросы преподавателя, которые могут выходить за рамки билетов, но в рамках изучаемого материала дисциплины.

После ответа на теоретический вопрос обучающийся приступает к решению задачи, гарантированно на решение задачи времени дается 30 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения, вопросы могут касаться всего материала изучаемой дисциплины.