ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказ ректора
от «7» июня 2021 г. № 78

Б1.О.45 Виртуальные частные сети

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – № 5 «Безопасность открытых информационных систем»
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – 5 лет 6 месяцев очная форма
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану (УП) – 180

Формы промежуточной аттестации в семестрах:
очная форма обучения:
экзамен 9

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	9	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в форме ПП*	**85**	**85**
– лекции	34	34
– практические (семинарские)	34	34
– лабораторные	17	17
Самостоятельная работа	**59**	**59**
Экзамен	**36**	**36**
Итого	**180**	**180**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – уровень специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация N 5 "Безопасность открытых информационных систем", утвержденным Приказом Минобрнауки России от 26.11.2020 г. № 1457.

Программу составил:
ст.преподаватель кафедры ИСиЗИ _____ Ю.О. Купитман

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11/2

И.о.зав. кафедрой, к.э.н, доцент _____ Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	формирование представления о криптографических протоколах и стандартах;
2	ознакомление обучающихся с основными техническими средствами построения виртуальных частных сетей.

1.2 Задачи дисциплины

1	ознакомление с основными понятиями в области криптографических протоколов и стандартов;
2	изучение основ построения виртуальных частных сетей (VPN);
3	ознакомление обучаемых с основными практическими приемами построения VPN;
4	рассмотрение различных вариантов и схем создания VPN;
5	ознакомиться со стандартными протоколами VPN и управлением криптографическими ключами в VPN.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота.

Задачи воспитательной работы с обучающимися:

– развитие мировоззрения и актуализация системы базовых ценностей личности;

– приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям;

– воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации;

– воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;

– обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;

– выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

Для успешного усвоения дисциплины «Виртуальные частные сети» необходимо, чтобы студент владел знаниями, умениями и навыки, сформированные в процессе изучения дисциплин Б1.О.47 «Информационные технологии», Б1.О.33 «Основы информационной безопасности», Б1.О.35 «Организация ЭВМ и вычислительных систем», Б1.О.36 «Сети и системы передачи информации», Б1.О.48 «Теоретические основы компьютерной безопасности», Б1.О.31 «Безопасность сетей ЭВМ» из цикла учебного плана по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация N 5 "Безопасность открытых информационных систем".

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б2.В.03(П) Производственная - проектно-технологическая
2	Б2.В.05(Пд) Производственная - преддипломная
3	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
4	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и	ОПК-9.1. Проводит анализ профессиональной деятельности для решения задач защиты информации, сетей и систем передачи данных	**Знать:** – методики оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов; – все основные современные ИТ, средства технической

тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.3. Знает основные информационные технологии, используемые в автоматизированных системах, их состояние и тенденции развития	защиты информации, сетей и систем передачи информации и тенденции их развития; – уровни защищённости автоматизированных систем; – принципы эксплуатации систем и средств обеспечения информационной безопасности в вычислительных системах; – основные протоколы и сервисы идентификации и аутентификации абонентов и объектов сети. **Уметь:** – применять на практике методики оценки защищенности автоматизированных систем; – составлять и организовывать на практике перечень работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; – составлять и организовывать на практике перечень работ по вводу в эксплуатацию сетей и систем передачи информации. **Владеть:** – навыками безопасного использования технических средств автоматизации; – навыками документирования оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов; – способностью формулировать принципы эксплуатации систем и средств обеспечения информационной безопасности; – методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности; – методами организации выполнения работ по вводу в эксплуатацию сетей и систем передачи информации.
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2. Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота	**Знать:** – российские и международные стандарты, описывающие криптографические функции; – стандартные криптопротоколы; – методы и средства организации защиты каналов связи и электронного документооборота; – **Уметь:** – определять перечень нормативных актов и руководящих документов по использованию криптографических протоколов; – проводить инструментальный мониторинг защищенности информации в VPN и выявлять каналы утечки информации **Владеть:** – навыками применения криптопротоколов и стандартов для построения защищенных систем и защиты электронного документооборота; – методами и средствами организации защиты каналов связи и электронного документооборота.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
	Введение. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Виды	9	1				ОПК-9.1 ОПК-9.3

	контроля знаний.						ОПК-10.2
1	**Раздел 1. Базовые сведения о технологиях обеспечении ИБ объектов**						
1.1	Состав и классификация средств обеспечения ИБ объектов. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов.	9	1	2	2	4	ОПК-9.1 ОПК-9.3 ОПК-10.2
2	**Раздел 2. Межсетевые экраны (МЭ)**						
2.1	Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.	9	4	4	1	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
2.2	Маршрутизаторы Cisco. Назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов ФПСУ-IP. Идентификация и аутентификация комплекса в сети. Удаленное администрирование. Построение VPN на базе комплекса. Комплекс ФПСУ-IP-клиент.	9	4	4	1	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
3	**Раздел 3. Виртуальные частные сети (VPN)**						
3.1	Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Специфика построения VPN. Критерии, предъявляемые к VPN. Политики безопасности для VPN.	9	2	4	2	4	ОПК-9.1 ОПК-9.3 ОПК-10.2
3.2	Туннелирование. Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.	9	4	2	1	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
3.3	Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, Client\Server VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP. Основные варианты создания VPN: защищенные, частные и промежуточные каналы.	9	4	2	1	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
3.4	Варианты политик безопасности при использовании каналов Internet для построения VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т.д. Варианты построения VPN. VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики, сравнительный анализ.	9	4	4	2	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
4	**Раздел 4. Стандартные протоколы создания VPN**						
4.1	Протокол PPTP Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее	9	2	4	2	6	ОПК-9.1 ОПК-9.3 ОПК-10.2

	соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000.						
4.2	Протокол L2TP Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола E2TP в среде Windows 2000.	9	2	4	2	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
4.3	Протокол IPSec Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция данных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, генерация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на соответствие записи в SPD) пакетов. Использование комбинированных криптографических алгоритмов в ESP. Особенности использования расширенных (64-битных) порядковых номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием протокола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования параметров безопасности IKE_SA и обмена по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Сообщения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т.д.). Форматы основного заголовка IKE и заголовков сообщений.	9	4	2	2	6	ОПК-9.1 ОПК-9.3 ОПК-10.2
5	**Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN)**						
5.1	Виды, протоколы и безопасность VLAN. VLAN с группировкой портов. VLAN с маркированными кадрами. VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN.	9	2	2	1	3	ОПК-9.1 ОПК-9.3 ОПК-10.2
	Подготовка к экзамену						
	Экзамен по дисциплине	9				36	

* Код индикатора достижения компетенции проставляется или для всего раздела или для каждой темы или для каждого вида работы.

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ

ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине: оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1.1	Пугин В.В., Голубничая Е.Ю., Лабада С.А.	Защита информации в компьютерных информационных системах: учебное пособие URL: https://e.lanbook.com/book/182299	Самара: ПГУТИ, 2018	100% онлайн
6.1.1.2	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник URL: https://biblioclub.ru/index.php?page=book&id=499170	Москва; Берлин: Директ-Медиа, 2019	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	А. В. Скрыпников, Д. В. Арапов, В. В. Денисенко, Т. Д. Герасимова	Защита Web-приложений: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=612405	Воронеж: Воронежский государственный университет инженерных технологий, 2020	100% онлайн
6.1.2.2	Шевченко В.П.	Вычислительные системы, сети и телекоммуникации URL: https://www.book.ru/book/936930	М.: КноРус, 2021	100% онлайн

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	Бизин Д. И., Коваленко О. Н.	Виртуальные частные сети (VPN): учебно-методическое пособие к выполнению лабораторных работ URL: https://e.lanbook.com/book/165629	Омск: ОмГУПС, 2019	100% онлайн

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.2.1	VPN: ещё раз просто о сложном URL: https://habr.com/ru/post/534250/
6.2.2	Технология VPN — определение, принципы использования и способы организации URL: https://eternalhost.net/blog/virtualnyj-server/chto-takoe-vpn
6.2.3	Лекция 11: Виртуальные частные сети URL: https://intuit.ru/studies/courses/102/102/lecture/2991?page=1
6.3 Программное обеспечение и информационные справочные системы	
6.3.1 Базовое программное обеспечение	
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №03341000100180000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №03341000100180000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org
6.3.2 Специализированное программное обеспечение	
6.3.2.1	Cisco Packet Tracer
6.3.3 Информационные справочные системы	
6.3.3.1	«Консультант +» http://www.consultant.ru/
6.3.3.2	«Техэксперт» http://www.cntd.ru/
6.4Правовые и нормативные документы	
6.4.1	Не предусмотрено программой

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины. Помещения для хранения и профилактического обслуживания учебного оборудования – А-521.
3	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
4	Учебная лаборатория Д-508 «Информационные системы и сетевые технологии». Оснащение лаборатории:14 ПЭВМ, сетевое и программное обеспечение.
5	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей

	области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. В конспект рекомендуется выписывать определения, формулировки и доказательства теорем, формулы и т.п. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий и наиболее часто употребляемые формулы дисциплины. К каждой лекции следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. При этом необходимо воспроизводить на бумаге все рассуждения, как имеющиеся в учебнике или конспекте, так и пропущенные в силу их простоты. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины. Особое внимание следует обращать на определение основных понятий дисциплины. Обучающийся должен подробно разбирать примеры, которые поясняют понятия
Самостоятельная работа	Обучение по дисциплине «Виртуальные частные сети» предусматривает активную самостоятельную работу обучающегося. На самостоятельную работу отводится 59 часов по очной форме обучения. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а так же указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения общих домашних заданий. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы, можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.О.45 Виртуальные частные сети

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – № 5 «Безопасность открытых информационных систем»

ИРКУТСК

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией Университета, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Виртуальные частные сети» участвует в формировании компетенций:

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации.

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
9 семестр					

1	1,2	Текущий контроль	Раздел 1. Базовые сведения о технологиях обеспечении ИБ объектов	ОПК-9.1 ОПК-9.3 ОПК-10.2	Собеседование (устно) Сообщение, доклад Защита лабораторной работы
2	3-5	Текущий контроль	Раздел 2. Межсетевые экраны (МЭ)	ОПК-9.1 ОПК-9.3 ОПК-10.2	Собеседование (устно) Сообщение, доклад Защита лабораторной работы
3	6-10	Текущий контроль	Раздел 3. Виртуальные частные сети (VPN)	ОПК-9.1 ОПК-9.3 ОПК-10.2	Собеседование (устно) Сообщение, доклад Защита лабораторной работы
4	11-14	Текущий контроль	Раздел 4. Стандартные протоколы создания VPN	ОПК-9.1 ОПК-9.3 ОПК-10.2	Собеседование (устно) Сообщение, доклад Защита лабораторной работы
5	15-17	Текущий контроль	Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN)	ОПК-9.1 ОПК-9.3 ОПК-10.2	Собеседование (устно) Сообщение, доклад Защита лабораторной работы
6	20-22	Промежуточная аттестация - экзамен	Раздел 1. Базовые сведения о технологиях обеспечении ИБ объектов. Раздел 2. Межсетевые экраны (МЭ). Раздел 3. Виртуальные частные сети (VPN). Раздел 4. Стандартные протоколы создания VPN. Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN).	ОПК-9.1 ОПК-9.3 ОПК-10.2	Тестирование Собеседование (устно)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины/прохождения практики включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» .

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1.	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение	Вопросы по темам/разделам дисциплины

		объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	
2.	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
3.	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4.	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
5.	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме или экзамена. Шкала оценивания уровня освоения компетенций

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Критерии и шкалы оценивания результатов обучения при проведении

текущего контроля успеваемости

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, электронный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, электронный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, электронный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, электронный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

Оценочное средство «Тест».

Тестирование с применением компьютерных технологий проводится по окончанию изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и опыта деятельности).

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации.

Промежуточная аттестация в форме экзамена – результаты тестирования могут являться допуском к экзамену:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен

Преподаватель вправе предусмотреть тесты для самоконтроля обучающихся по разделам дисциплины, сформировав их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Перечень теоретических вопросов к экзамену

1. Различные подходы к определению VPN.
2. Цели и задачи применения VPN-технологий.
3. Механизм туннелирования как основа построения VPN.
4. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования.
5. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.
6. Обработка входящих и исходящих пакетов.
7. Классификация VPN компании Check Point по типу устанавливаемых соединений. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности
8. VPN в сетях общего пользования.
9. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP
10. Функции протокола PPTP. Компоненты PPTP. Сценарии работы протокола.
11. Архитектура PPTP. Протокол L2TP: основные функции и характеристики протокола.
12. Управление L2TP-туннелем
13. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec
14. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec
15. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов

16. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP

17. Использование комбинированных криптографических алгоритмов в ESP

18. Что такое криптографический ключ

19. Виды криптографических ключей

20. Процедуры использования ключей

21. Средство построения VPN АПКШ «Континент»

22. Средство построения VPN ViPNet

23. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования.

24. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных.

25. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec.

26. Функции протокола PPTP. Компоненты PPTP. Сценарии работы протокола.

27. Архитектура PPTP.

28. Протокол L2TP: основные функции и характеристики протокола.

29. Управление L2TP-туннелем.

30. Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec.

31. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec.

32. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов.

33. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP.

3.2 Перечень практических вопросов к экзамену

1. Последовательно напишите консольные команды, которые нужно ввести в CLI маршрутизатора для присвоения IP-адреса интерфейсу.
2. Перечислите три способа создания VLAN на коммутаторе с написанием команд.
3. Перечислите отличия проводов Cupper Cross-Over и Cupper Stright. Как они представлены в Cisco Packet Tracer?
4. Перечислите все семь уровней эталонной модели OSI. Расскажите, на каком уровне работает точка доступа, на каком маршрутизатор и на каком коммутатор. Какие данные передаются на каждом уровне?
5. Последовательно опишите действия для подключения к сетевому оборудованию через консоль.
6. Последовательно опишите действия, выполняемые при настройке SSH.
7. Последовательно опишите действия, выполняемые при настройке IPSec.
8. Напишите команду, которой можно проверить работоспособность VPN по IPSec.

3.3 Тестирование по дисциплине

3.3.1 Структура и образец типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
Раздел 1. Базовые сведения о технологиях обеспечении ИБ объектов	1.1. Состав и классификация средств обеспечения ИБ объектов. Место технологии построения виртуальных сетей в общей системе средств обеспечения ИБ объектов.	3 - тип А 3 - тип В 2 - тип С
	Итого по разделу	∑ 8 3 - тип А 3 - тип В 2 - тип С
Раздел 2. Межсетевые экраны (МЭ)	2.1. Назначение и функции МЭ. Основные компоненты МЭ. Принцип работы МЭ, варианты позиционирования МЭ. Руководящий документ Гостехкомиссии РФ по МЭ. Профили защиты для МЭ. Основные типы МЭ: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, МЭ экспертного уровня. Персональные МЭ. Основные компоненты МЭ. Слабости МЭ. Выбор реализаций МЭ.	6 - тип А 6 - тип В 5 - тип С
	2.2. Маршрутизаторы Cisco. Назначение и основные характеристики. Операционная система. Интерфейсы маршрутизаторов. Основные разделы и подразделы меню комплекса межсетевых экранов ФПСУ-IP. Идентификация и аутентификация комплекса в сети. Удаленное администрирование. Построение VPN на базе комплекса. Комплекс ФПСУ-IP-клиент.	7 - тип А 8 - тип В 4 - тип С
	Итого по разделу	∑ 36 13 – тип А 14 – тип В 9 – тип С
Раздел 3. Виртуальные частные сети (VPN)	3.1 Различные подходы к определению VPN, определение компании Check Point Software Technologies. Цели и задачи применения VPN-технологий. Преимущества VPN по сравнению с защищенными выделенными каналами связи и другими методами организации защищенной связи. Специфика построения VPN. Критерии, предъявляемые к VPN. Политики безопасности для VPN.	3 - тип А 4 - тип В 3 - тип С
	3.2 Туннелирование. Механизм туннелирования как основа построения VPN. Общий поход к созданию туннелей, функции конкретных протоколов, участвующих в процессе туннелирования. Обеспечение конфиденциальности, подлинности и целостности при использовании инкапсуляции данных. Базовая схема VPN. VPN-агенты. Функции VPN-агентов. Обработка входящих и исходящих пакетов. Различные варианты позиционирования и использования VPN-агентов.	3 - тип А 3 - тип В 3 - тип С
	3.3 Классификация VPN компании Check Point по типу устанавливаемых соединений: Intranet VPN, Client\Server VPN, Extranet VPN, Remote Access VPN – определения, характерные черты и особенности использования. Классификация VPN согласно консорциуму VPN (VPNC) по степени защищенности: доверенные, защищенные и смешанные VPN – определения, требования, технологии построения. VPN в сетях общего пользования. Специфика использования VPN в сетях Frame Realay, ATM, X.25, TCP/IP. Основные варианты создания VPN: защищенные, частные и промежуточные каналы.	3 - тип А 4 - тип В 3 - тип С
	3.4 Варианты политик безопасности при использовании каналов Internet для построения VPN. Интеграция VPN и дополнительных средств защиты: использование PKI, криптографические модули, аудит, антивирусные средства и т.д. Варианты построения VPN. VPN на базе сетевой ОС, МЭ, маршрутизаторов, специализированного ПО, аппаратных средств – основные характеристики, сравнительный анализ.	2 - тип А 4 - тип В 3 - тип С

	Итого по разделу	∑ 38 11 – тип А 15 – тип В 12 – тип С
Раздел 4. Стандартные протоколы создания VPN	4.1 Протокол PPTP Функции протокола. Компоненты PPTP. Сценарии работы протокола. Архитектура PPTP. Управляющее соединение и управляющие сообщения. Инкапсуляция данных при передаче. Аутентификация, контроль доступа и шифрование. Настройка VPN на базе протокола PPTP в среде Windows 2000.	6 - тип А 4 - тип В 3 - тип С
	4.2 Протокол L2TP Основные функции и характеристики протокола. Управление L2TP-туннелем. Управляющие сообщения L2TP. L2TP /IPSec инкапсуляция данных. Обработка входящих и исходящих данных. Настройка VPN на базе протокола E2TP в среде Windows 2000.	5 - тип А 4 - тип В 2 - тип С
	4.3 Протокол IPSec Архитектура IPSec. Функции, принцип работы, сценарии применения IPSec. Обзор основных компонентов IPSec. Главные базы данных IPSec: SPD, SAD, PAD. Политики безопасности IPSec. Ассоциации безопасности (SA): определение, назначение, процедуры управления. Обработка IP-трафика. Особенности обработки ICMP-трафика и фрагментированных IP-пакетов. Использование аудита в архитектуре IPSec. Защита данных с помощью протоколов AH и ESP. Инкапсуляция данных в транспортном и туннельном режимах работы. Форматы заголовков. Защищаемые поля IP-заголовка при использовании AH в транспортном режиме. Обработка исходящих (поиск SA, генерация порядкового номера, вычисление ICV и шифрование данных, фрагментация) и входящих (сборка, поиск SA, проверка порядкового номера, проверка ICV, расшифрование, проверка на соответствие записи в SPD) пакетов. Использование комбинированных криптографических алгоритмов в ESP. Особенности использования расширенных (64-битных) порядковых номеров. Защита от повторной передачи пакетов. Согласование параметров безопасности с использованием протокола IKE. Порядок обмена сообщениями IKE. Сообщения IKE_SA_INIT для согласования параметров безопасности IKE_SA и обмена по протоколу Диффи-Хеллмана. Сообщения IKE_AUTH для аутентификации и установления CHILD_SA для защиты данных с помощью AH или ESP. Сообщения CREATE_CHILD_SA для согласования дополнительных CHILD_SA в рамках данной IKE_SA. Сообщения INFORMATIONAL для сообщения информации о текущем состоянии или ошибках. Детали работы протокола (согласование версий протокола, использование порядковых номеров, генерирование ключевого материала, обработка ошибок и т.д.). Форматы основного заголовка IKE и заголовков сообщений.	6 - тип А 5 - тип В 3 - тип С
	Итого по разделу	∑ 36 15 – тип А 13 – тип В 8 – тип С
Раздел 5. Базовые сведения о виртуальных локальных сетях (VLAN)	5.1 Виды, протоколы и безопасность VLAN VLAN с группировкой портов. VLAN с маркированными кадрами. VLAN на основе протоколов высокого уровня. Этапы перехода к VLAN. Протокол VTP. Безопасность в VLAN. Преимущества VLAN.	16 - тип А 12 - тип В 8 - тип С
	Итого по разделу	∑ 36 16 - тип А 12 - тип В 8 - тип С

Итого по дисциплине	**∑ 154** **58 – тип А** **57 – тип В** **39 – тип С**

Образец типового итогового теста по дисциплине за весь период ее освоения

Описание требований к тесту: обучающемуся предъявляются 20 тестовых вопросов, которые необходимо решить за 30 минут. Пользоваться телефонами, лекциями, теоретическими материалами из лабораторных работ нельзя.

Образец типового теста содержит задания для оценки знаний, для оценки умений, для оценки навыков и (или) опыта деятельности.

1. SSH расшифровывается как:
   a) secure shell
   b) shell of secure
   c) security service host
   d) security system host

2. VLAN расшифровывается как:
   a) valid local authentication network
   b) virtual local area network
   c) virtual linear authentication network
   d) valuable local advance network

3. Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами, называется _____.

4. Напишите команду, которой можно вывести текущие ssh соединения.

5. Установите соответствие между термином и его определением.

1. Коммутатор	a. Базовая станция, предназначенная для обеспечения беспроводного доступа к уже существующей сети или создания новой беспроводной сети.
2. Повторитель	b. Сетевое оборудование, предназначенное для увеличения расстояния сетевого соединения и его расширения за пределы одного сегмента или для организации двух ветвей
3. Маршрутизатор	c. Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети
4. Точка доступа	d. Специализированное устройство, которое пересылает пакеты между различными сегментами сети

1. _____
2. _____
3. _____
4. _____

6. Расскажите, что такое ПАК ФПСУ-IP.

7. Выберите протоколы туннелирования, используемые в VPN:
   a) SMTP
   b) L2TP
   c) TCP
   d) FTP
   e) Telnet

f) PPTP
g) HTTP
h) IPSec

8. Специальная технология, определяющая способ упаковки, передачи и распаковки данных при передаче по VPN-соединению, называется _____.

9. Включение всего пакета одного протокола внутрь пакета другого протокола в качестве передаваемой информации, это…
a) декапсуляция;
b) инкапсуляция;
c) коммутация;
d) виртуализация.

10. Выберите протоколы, составляющие ядро IPSec:
a) IEEE 802.1q
b) TCP
c) ESP
d) AH
e) OSPF
f) SSH
g) DNS
h) IKE
i) SMTP

11. Можно ли межсетевой экран назвать Firewall?
a) да
b) нет
c) затрудняюсь ответить

12. Установите соответствие между режимами работы и их описанием в Cisco IOS:

1. Пользовательский режим	a. доступны команды, позволяющие получить полную информацию о конфигурации оборудования и его состоянии
2. Привилегированный режим	d. доступны команды конфигурирования оборудования и команды перехода в режимы конфигурирования его подсистем
3. Конфигурационный режим	b. доступны только простые команды, не влияющие на конфигурацию оборудования.

1. _____
2. _____
3. _____

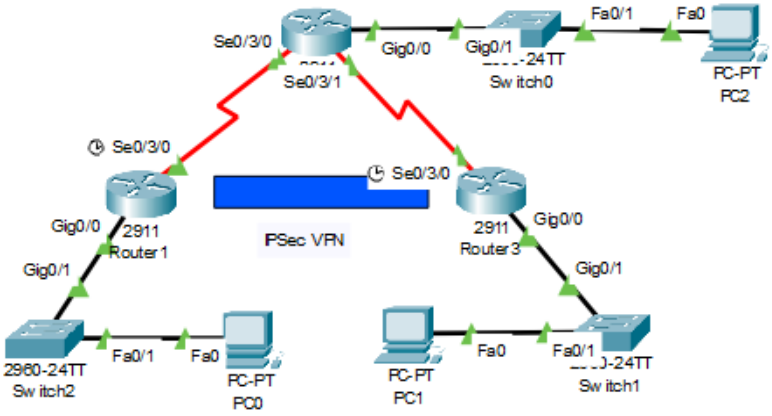
13. Установите соответствие между режимами работы и приглашением командной строки в Cisco IOS:

1. Пользовательский режим	a. Router(config)#
2. Привилегированный режим	d. Router>
3. Конфигурационный режим	b. Router#

1. _____
2. _____
3. _____

14. Напишите консольную команду присвоения IP-адреса интерфейсу маршрутизатора.
15. Внимательно рассмотрите рисунок.

15.1 При настроенном туннелировании между R1 и R3 будет ли R2, находящийся между ними, видеть зашифрованный траффик?



a) да
b) нет
c) затрудняюсь ответить

15.2. Будет ли настроенный VPN препятствовать маршрутизации внутри сети от PC0 до PC2 или от PC0 до PC3?

a) да
b) нет
c) затрудняюсь ответить

16. Напишите два режима работы протокола IPSec.
17. Расскажите, какую информацию выведет команда:

```
R1# show crypto ipsec sa
```

18. Каким образом настроить L2-коммутатор, чтобы к нему можно было подключиться через SSH?

a) настроить SVI и задать ему IP-адрес как обычному интерфейсу
b) настроить VTY и задать ему IP-адрес как обычному интерфейсу
c) задать обычному интерфейсу коммутатора IP-адрес
d) коммутаторы L2-уровня невозможно настроить для SSH
e) затрудняюсь ответить

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины/практики.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование – это форма проведения устного зачета по каждому разделу дисциплины. Также может проводиться лабораторной работе с целью выявления степени готовности обучающихся по тем или иным разделам дисциплины. После предварительной подготовки студент излагает преподавателю своё видение вопроса. Преподаватель задаёт уточняющие и дополнительные вопросы, а затем сообщает студенту своё решение об его промежуточной аттестации.

Сообщение, доклад	Обучаемый получает от преподавателя тему доклада и представляет его в устной форме на семинаре. Следует продемонстрировать авторскую позицию, самостоятельный взгляд на вопрос, показать изучение достаточного количества источников с их авторским анализом. Приветствуется дискуссионность материала.
Тест	Тестирование с применением компьютерных технологий проводится в течение семестра и по завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности). Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам каждого семестра и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа. Результаты тестирования могут быть использованы при проведении промежуточной аттестации, как в форме зачета, так и в форме экзамена. Тесты для самоконтроля обучающихся по разделам дисциплины сформированы из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом.
Защита лабораторной работы	Защита лабораторной работы как средство контроля практических знаний проводится на лабораторных занятиях. Темы лабораторных работ определены в рабочей программе дисциплины. Преподаватель для каждой лабораторной работы выдает методическое указание, содержащее тему лабораторной работы, цель работы и задание. Обучающийся должен в отведенное время провести необходимые действия, оформить отчет по лабораторной работе и защитить отчет (протокол) преподавателю вместе с демонстрацией работоспособной сети. Защита осуществляется путем доклада обучающегося преподавателю о выполненной работе, выводах и заключениях. Доклад иллюстрируется материалами отчета. Также обучающийся демонстрирует работоспособную настроенную по заданию сеть, выполненную в программном продукте CPT, либо же на реальном оборудовании. Обучающийся обязан отвечать на дополнительные вопросы преподавателя, которые могут возникнуть в ходе доклада. Оценка (зачтено/не зачтено) защиты лабораторной работы объявляется обучающемуся сразу после защиты.

Для организации и проведения промежуточной аттестации (в форме экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

– перечень теоретических вопросов к экзамену для оценки знаний;

– перечень типовых практических вопросов к экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических вопросов разного уровня сложности к экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду

ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

Образец экзаменационного билета

ИРГУПС 2021-20212 учебный год	**Экзаменационный билет № 1** **по дисциплине «Виртуальные частные сети»** **Специализация 10.05.03 Информационная безопасность автоматизированных систем** **9 семестр**	Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС Кириллова Т.К.
1. Протокол L2TP: основные функции и характеристики протокола. 2. VPN в сетях общего пользования. 3. Последовательно напишите консольные команды, которые нужно ввести в CLI маршрутизатора для присвоения IP-адреса интерфейсу. Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			
1	Электронно-библиотечная система «Znanium.com», https://znanium.com/ заменена на Электронно-библиотечную систему «BOOK.ru», https://www.book.ru/			10	10	приказ от 13.01.2022 №23-1		21.01.2022
	6	6.1	6.1.2					