Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
01 06 2021 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине **«Защита информации от несанкционированного доступа»**
для основной профессиональной образовательной программы по направлению
11.03.02 «Инфокоммуникационные технологии и системы связи»
направленность (профиль) – Инфокоммуникационные технологии в услугах связи
квалификация – бакалавр
форма обучения – очная
год начала подготовки (по учебному плану) – 2021

Екатеринбург 2021

Приложение 1 к рабочей программе
по дисциплине «Защита информации от несанкционированного доступа»

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
« ____ » _____ 2021 г.

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине **«Защита информации от несанкционированного доступа»**
для основной профессиональной образовательной программы по направлению
11.03.02 «Инфокоммуникационные технологии и системы связи»
направленность (профиль) – Инфокоммуникационные технологии в услугах связи
квалификация – бакалавр
форма обучения – очная
год начала подготовки (по учебному плану) – 2021

Екатеринбург 2021

1. Перечень компетенций и индикаторов их достижения

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенций	Этап	Предшествующие этапы (с указанием дисциплин)
ПК-1 – Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных	**ПК-1.1** Знает принципы построения и работы сети связи, протоколов обмена информацией и сигнализации, используемых в сетях связи, стандарты качества передачи данных и голоса. **ПК-1.2** Знает законодательство Российской Федерации в области связи, предоставления услуг связи. **ПК-1.3** Знает основы технической эксплуатации, принципы построения и работы коммутационного оборудования коммутационных подсистем и сетевых платформ, перспективы технического развития отрасли связи **ПК-1.4** Умеет собирать и анализировать данные о работе сети, статистические параметры трафика; проводить расчет интерфейсов внутренних направлений сети; вырабатывать решения по оперативному переконфигурированию сети, изменению параметров коммутационной подсистемы, сетевых платформ; изменять параметры коммутационной подсистемы, маршрутизации трафика, организации новых и расширении имеющихся направлений связи. **ПК-1.5** Умеет эксплуатировать оборудование коммутационной подсистемы, сопутствующего оборудования и сетевых платформ. **ПК-1.6** Владеет навыками разработки схемы организации связи, построения и расширения коммутационной подсистемы и сетевых платформ, навыками работы с базами данных и администрирования оборудования коммутационной подсистемы.	8	Основы теории цепей (1 этап), ЭВМ и периферийные устройства (3 этап), Вычислительная техника и информационные технологии (3 этап), Элементная база телекоммуникационных систем (3 этап), Языки программирования (4 этап), Программирование сетевых приложений (4 этап), Схемотехника телекоммуникационных устройств (4 этап), Базы данных в телекоммуникациях (4 этап), Теория связи (4 этап), Сетевые технологии высокоскоростной передачи данных (5 этап), Направляющие среды электросвязи (5 этап), Администрирование в инфокоммуникационных системах (6 этап), Операционные системы (6 этап), Архитектура и программное обеспечение сетевых инфокоммуникационных устройств (6 этап), Корпоративные инфокоммуникационные системы и услуги (6 этап), Системы сетевого сопровождения инфокоммуникационных систем и услуг (6 этап), Цифровые системы распределения сообщений (6 этап), Теория телетрафика (7 этап), Проектирование и эксплуатация сетей связи (7 этап), Электропитание устройств и систем телекоммуникаций (6 этап), Пакетные радиосети (6 этап),

			Сети и системы мобильной связи (6 этап).
ПК-8 - Способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных	**ПК-8.1** Знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети; установку и эксплуатацию администрируемых сетевых устройств, установке и эксплуатация администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Модель ISO для управления сетевым трафиком; Модели IEEE; Модели информационно-телекоммуникационной сети "Интернет"; Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе. **ПК-8.2** Умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры администрируемой сети; Использовать современные средства администрирования баз данных; **ПК-8.3** Владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения **ПК-8.5** Владеет навыками планирования стратегии восстановления сетевой системы и программного обеспечения инфокоммуникационной системы	8	Программирование сетевых приложений (4 этап), Схемотехника телекоммуникационных устройств (4 этап), Базы данных в телекоммуникациях (4 этап), Теория связи (4 этап), Сетевые технологии высокоскоростной передачи данных (5 этап), Направляющие среды электросвязи (5 этап), Администрирование в инфокоммуникационных системах (6 этап), Операционные системы (6 этап), Архитектура и программное обеспечение сетевых инфокоммуникационных устройств (6 этап), Корпоративные инфокоммуникационные системы и услуги (6 этап), Системы сетевого сопровождения инфокоммуникационных систем и услуг (6 этап), Пакетные радиосети (6 этап), Нормативно-правовая база профессиональной деятельности (7 этап).

Форма(ы) промежуточной аттестации по дисциплине: экзамен (8 семестр).

2. Показатели, критерии и шкалы оценивания компетенций

2.1 Показателем оценивания компетенций на этапе их формирования при изучении дисциплины является уровень их освоения.

Шкала оценивания	Результаты обучения	Дескрипторы уровней освоения компетенций
ПК-1 – Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных		
Низкий (пороговый) уровень	**ПК-1.1** Знает принципы построения и работы сети связи, протоколов обмена информацией и сигнализации, используемых в сетях связи, стандарты качества передачи данных и голоса. **ПК-1.2** Знает законодательство Российской Федерации в области связи, предоставления услуг связи. **ПК-1.3** Знает основы технической эксплуатации, принципы построения и работы коммутационного оборудования коммутационных подсистем и сетевых платформ, перспективы технического развития отрасли связи	При ответе на вопросы допускает значительные ошибки, не в полной мере связывает теоретические и практические вопросы по методам защита сетей от несанкционированного доступа, используемого оборудования и настройки системы защиты сетей. Допускает ошибки при решении практических задач.
	ПК-1.4 Умеет собирать и анализировать данные о работе сети, статистические параметры трафика; проводить расчет интерфейсов внутренних направлений сети; вырабатывать решения по оперативному переконфигурированию сети, изменению параметров коммутационной подсистемы, сетевых платформ; изменять параметры коммутационной подсистемы, маршрутизации трафика, организации новых и расширении имеющихся направлений связи **ПК-1.5** Умеет эксплуатировать оборудование коммутационной подсистемы, сопутствующего оборудования и сетевых платформ	Допускается ошибки при выборе оборудования и инструментов для защиты от несанкционированного доступа. Допускает ошибки в настройках защиты сетей от несанкционированного доступа.
	ПК-1.6 Владеет навыками разработки схемы организации связи, построения и расширения коммутационной подсистемы и сетевых платформ, навыками работы с базами данных и администрирования оборудования коммутационной подсистемы	Допускает значительные ошибки в проектировании систем защиты сетей от несанкционированного доступа.
Средний уровень	**ПК-1.1** Знает принципы построения и работы сети связи,	При ответе на вопросы допускает не значительные ошибки, в полной мере

	протоколов обмена информацией и сигнализации, используемых в сетях связи, стандарты качества передачи данных и голоса. **ПК-1.2** Знает законодательство Российской Федерации в области связи, предоставления услуг связи. **ПК-1.3** Знает основы технической эксплуатации, принципы построения и работы коммутационного оборудования коммутационных подсистем и сетевых платформ, перспективы технического развития отрасли связи	связывает теоретические и практические вопросы по методам защита сетей от несанкционированного доступа, используемого оборудования и настройки системы защиты сетей. Допускает не значительные ошибки при решении практических задач.
	ПК-1.4 Умеет собирать и анализировать данные о работе сети, статистические параметры трафика; проводить расчет интерфейсов внутренних направлений сети; вырабатывать решения по оперативному переконфигурированию сети, изменению параметров коммутационной подсистемы, сетевых платформ; изменять параметры коммутационной подсистемы, маршрутизации трафика, организации новых и расширении имеющихся направлений связи **ПК-1.5** Умеет эксплуатировать оборудование коммутационной подсистемы, сопутствующего оборудования и сетевых платформ	Допускает при выборе оборудования и инструментов для защиты от несанкционированного доступа. Допускает не значительные ошибки в настройках защиты сетей от несанкционированного доступа.
	ПК-1.6 Владеет навыками разработки схемы организации связи, построения и расширения коммутационной подсистемы и сетевых платформ, навыками работы с базами данных и администрирования оборудования коммутационной подсистемы	Допускает не значительные ошибки в проектировании систем защиты сетей от несанкционированного доступа.
Высокий уровень	**ПК-1.1** Знает принципы построения и работы сети связи, протоколов обмена информацией и сигнализации, используемых в сетях связи, стандарты качества передачи данных и голоса. **ПК-1.2** Знает законодательство Российской Федерации в области связи, предоставления услуг связи. **ПК-1.3** Знает основы технической эксплуатации, принципы	При ответе на вопросы не допускает ошибок, в полной мере связывает теоретические и практические вопросы по методам защита сетей от несанкционированного доступа, используемого оборудования и настройки системы защиты сетей. Не допускает ошибок при решении практических задач.

	построения и работы коммутационного оборудования коммутационных подсистем и сетевых платформ, перспективы технического развития отрасли связи	
	ПК-1.4 Умеет собирать и анализировать данные о работе сети, статистические параметры трафика; проводить расчет интерфейсов внутренних направлений сети; вырабатывать решения по оперативному переконфигурированию сети, изменению параметров коммутационной подсистемы, сетевых платформ; изменять параметры коммутационной подсистемы, маршрутизации трафика, организации новых и расширении имеющихся направлений связи **ПК-1.5** Умеет эксплуатировать оборудование коммутационной подсистемы, сопутствующего оборудования и сетевых платформ	Не допускает ошибок при выборе оборудования и инструментов для защиты от несанкционированного доступа, а также безошибочно настраивает защиту сетей от несанкционированного доступа.
	ПК-1.6 Владеет навыками разработки схемы организации связи, построения и расширения коммутационной подсистемы и сетевых платформ, навыками работы с базами данных и администрирования оборудования коммутационной подсистемы	Полностью владеет навыками проектирования систем защиты сетей от несанкционированного доступа.
ПК-8 - Способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных		
Низкий (пороговый) уровень	**ПК-8.1** Знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети; установку и эксплуатацию администрируемых сетевых устройств, установке и эксплуатация администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Модель ISO для управления сетевым трафиком; Модели IEEE; Модели информационно-	Допускает значительные ошибки при работе с ПК и в сети передачи данных, плохо ориентируется в программных пакетах, используемых для моделирования сетей связи.

	телекоммуникационной сети "Интернет"; Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе.	
	ПК-8.2 Умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры администрируемой сети; Использовать современные средства администрирования баз данных;	Допускает значительные ошибки при работе с ПК и в сети передачи данных. Допускает существенные ошибки при моделировании сетей связи.
	ПК-8.3 Владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения **ПК-8.5** Владеет навыками планирования стратегии восстановления сетевой системы и программного обеспечения инфокоммуникационной системы	Плохо ориентируется в методах диагностики аппаратного и программного обеспечения инфокоммуникационных систем. Не достаточно владеет навыками восстановления инфокоммуникационных систем при различных видах сетевых атак.
Средний уровень	**ПК-8.1** Знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети; установку и эксплуатацию администрируемых сетевых устройств, установке и эксплуатация администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Модель ISO для управления сетевым трафиком; Модели IEEE; Модели информационно-телекоммуникационной сети "Интернет"; Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе.	Допускает не значительные ошибки при работе с ПК и в сети передачи данных, хорошо ориентируется в программных пакетах, используемых для моделирования сетей связи.
	ПК-8.2 Умеет использовать современные стандарты при администрировании устройств и	Допускает не значительные ошибки при работе с ПК и в сети передачи данных. Допускает не существенные ошибки при

	программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры администрируемой сети; Использовать современные средства администрирования баз данных;	моделировании сетей связи.
	ПК-8.3 Владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения **ПК-8.5** Владеет навыками планирования стратегии восстановления сетевой системы и программного обеспечения инфокоммуникационной системы	Хорошо ориентируется в методах диагностики аппаратного и программного обеспечения инфокоммуникационных систем. Владеет навыками восстановления инфокоммуникационных систем при различных видах сетевых атак.
Высокий уровень	**ПК-8.1** Знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети; установку и эксплуатацию администрируемых сетевых устройств, установке и эксплуатация администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Модель ISO для управления сетевым трафиком; Модели IEEE; Модели информационно-телекоммуникационной сети "Интернет"; Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе.	Грамотно работает с ПК и в сети передачи данных, хорошо ориентируется в программных пакетах, используемых для моделирования сетей связи.
	ПК-8.2 Умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры администрируемой сети; Использовать современные средства администрирования баз данных;	Грамотно работает с ПК и в сети передачи данных, хорошо ориентируется в программных пакетах. Не допускает ошибок при моделировании сетей связи.

	ПК-8.3 Владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения **ПК-8.5** Владеет навыками планирования стратегии восстановления сетевой системы и программного обеспечения инфокоммуникационной системы	Хорошо ориентируется в методах диагностики аппаратного и программного обеспечения инфокоммуникационных систем. Владеет навыками восстановления инфокоммуникационных систем при различных видах сетевых атак.

2.2 Таблица соответствия результатов промежуточной аттестации по дисциплине уровню этапа формирования компетенций

Форма контроля	Шкала оценивания	Код индикатора достижения компетенций	Уровень освоения компетенции
Зачет по лабораторным и практическим работам	Зачёт	ПК-1.1	средний
		ПК-1.2	низкий
		ПК-1.3	средний
		ПК-1.4	высокий
		ПК-1.5	высокий
		ПК-1.6	средний
		ПК-8.1	средний
		ПК-8.2	средний
		ПК-8.3	средний
		ПК-8.4	средний
Экзамен	Удовлетворительно	ПК-1.1	средний
		ПК-1.2	низкий
		ПК-1.3	средний
		ПК-1.4	низкий
		ПК-1.5	низкий
		ПК-1.6	низкий
		ПК-8.1	средний
		ПК-8.2	низкий
		ПК-8.3	низкий
		ПК-8.5	низкий
	Хорошо	ПК-1.1	высокий
		ПК-1.2	низкий
		ПК-1.3	средний
		ПК-1.4	средний
		ПК-1.5	средний
		ПК-1.6	средний
		ПК-8.1	высокий
		ПК-8.2	средний
		ПК-8.3	средний
		ПК-8.5	средний
	Отлично	ПК-1.1	высокий
		ПК-1.2	средний
		ПК-1.3	высокий
		ПК-1.4	средний
		ПК-1.5	средний
		ПК-1.6	высокий
		ПК-8.1	высокий

		ПК-8.2	средний
		ПК-8.3	средний
		ПК-8.5	средний

3. Методические материалы, определяющие процедуры оценивания

Процесс оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, представлен в таблицах по формам обучения:

Тип занятия	Тема (раздел)	Оценочные средства
ПК-1.1 Знает принципы построения и работы сети связи, протоколов обмена информацией и сигнализации, используемых в сетях связи, стандарты качества передачи данных и голоса		
Лекция	Сетевые угрозы	Экзамен
	Общие принципы защиты от сетевых атак	Экзамен
	Защита сетевых устройств от несанкционированного доступа	Экзамен
	Аутентификация, авторизация и учет	Экзамен
	Защита сетей на канальном уровне	Экзамен
	Защита сетей на основе списков контроля доступа	Экзамен
	Виртуальные частные сети	Экзамен
	Организация сетевой безопасности на межсетевых экранах	Экзамен
	Защита оконечных устройств сетей	Экзамен
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Практическое занятие	Изучение принципов управления конфигурацией и образами IOS	Отчет по практическому занятию
	Поиск и устранение неисправностей в обеспечении безопасности сетей передачи данных	Отчет по практическому занятию
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену

	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-1.2 Знает законодательство Российской Федерации в области связи, предоставления услуг связи		
Лекция	Сетевые угрозы	Экзамен
	Общие принципы защиты от сетевых атак	Экзамен
	Защита сетевых устройств от несанкционированного доступа	Экзамен
	Аутентификация, авторизация и учет	Экзамен
	Защита сетей на канальном уровне	Экзамен
	Защита сетей на основе списков контроля доступа	Экзамен
	Виртуальные частные сети	Экзамен
	Организация сетевой безопасности на межсетевых экранах	Экзамен
	Защита оконечных устройств сетей	Экзамен
ПК-1.3 Знает основы технической эксплуатации, принципы построения и работы коммутационного оборудования коммутационных подсистем и сетевых платформ, перспективы технического развития отрасли связи		
Лекция	Сетевые угрозы	Экзамен
	Общие принципы защиты от сетевых атак	Экзамен
	Защита сетевых устройств от несанкционированного доступа	Экзамен
	Аутентификация, авторизация и учет	Экзамен
	Защита сетей на канальном уровне	Экзамен
	Защита сетей на основе списков контроля доступа	Экзамен
	Виртуальные частные сети	Экзамен
	Организация сетевой безопасности на межсетевых экранах	Экзамен
	Защита оконечных устройств сетей	Экзамен
	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе

Лабораторная работа	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Практическое занятие	Изучение принципов управления конфигурацией и образами IOS	Отчет по практическому занятию
	Поиск и устранение неисправностей в обеспечении безопасности сетей передачи данных	Отчет по практическому занятию
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-1.4 Умеет собирать и анализировать данные о работе сети, статистические параметры трафика; проводить расчет интерфейсов внутренних направлений сети; вырабатывать решения по оперативному переконфигурированию сети, изменению параметров коммутационной подсистемы, сетевых платформ; изменять параметры		

коммутационной подсистемы, маршрутизации трафика, организации новых и расширении имеющихся направлений связи		
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Практическое занятие	Изучение принципов управления конфигурацией и образами IOS	Отчет по практическому занятию
	Поиск и устранение неисправностей в обеспечении безопасности сетей передачи данных	Отчет по практическому занятию
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям

	Подготовка к экзамену	Экзамен
ПК-1.5 Умеет эксплуатировать оборудование коммутационной подсистемы, сопутствующего оборудования и сетевых платформ		
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-1.6 Владеет навыками разработки схемы организации связи, построения и расширения коммутационной подсистемы и сетевых платформ, навыками работы с базами данных и администрирования оборудования коммутационной подсистемы		
Лекции	Сетевые угрозы	Экзамен

	Общие принципы защиты от сетевых атак	Экзамен
	Защита сетевых устройств от несанкционированного доступа	Экзамен
	Аутентификация, авторизация и учет	Экзамен
	Защита сетей на канальном уровне	Экзамен
	Защита сетей на основе списков контроля доступа	Экзамен
	Виртуальные частные сети	Экзамен
	Организация сетевой безопасности на межсетевых экранах	Экзамен
	Защита оконечных устройств сетей	Экзамен
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Практическое занятие	Изучение принципов управления конфигурацией и образами IOS	Отчет по практическому занятию
	Поиск и устранение неисправностей в обеспечении безопасности сетей передачи данных	Отчет по практическому занятию
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе

	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-8.1 Знает архитектуру и общие принципы функционирования, аппаратных, программных и программно-аппаратных средств администрируемой сети; установку и эксплуатацию администрируемых сетевых устройств, установке и эксплуатация администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Модель ISO для управления сетевым трафиком; Модели IEEE; Модели информационно-телекоммуникационной сети "Интернет"; Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе.		
Лекция	Сетевые угрозы	Экзамен
	Общие принципы защиты от сетевых атак	Экзамен
	Защита сетевых устройств от несанкционированного доступа	Экзамен
	Аутентификация, авторизация и учет	Экзамен
	Защита сетей на канальном уровне	Экзамен
	Защита сетей на основе списков контроля доступа	Экзамен
	Виртуальные частные сети	Экзамен
	Организация сетевой безопасности на межсетевых экранах	Экзамен
	Защита оконечных устройств сетей	Экзамен
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Практическое занятие	Изучение принципов управления конфигурацией и образами IOS	Отчет по практическому занятию
	Поиск и устранение неисправностей в обеспечении безопасности сетей передачи данных	Отчет по практическому занятию
Самостоятельная	Проработка лекций	Экзамен

работа	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-8.2 Умеет использовать современные стандарты при администрировании устройств и программного обеспечения; применять штатные и внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры администрируемой сети; Использовать современные средства администрирования баз данных;		
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену

	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-8.3 Владеет навыками диагностики отказов и ошибок сетевых устройств и программного обеспечения		
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и

		практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе
	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен
ПК-8.5 Владеет навыками планирования стратегии восстановления сетевой системы и программного обеспечения инфокоммуникационной системы		
Лабораторная работа	Исследование методов защиты сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе
	Настройка сетевой безопасности с помощью функции Port Security	Отчет по лабораторной работе
	Исследование принципов организации защиты сетей с использованием VLAN	Отчет по лабораторной работе
	Исследование принципов настройки стандартных ACL	Отчет по лабораторной работе
	Исследование принципов настройки службы NAT	Отчет по лабораторной работе
	Исследование принципов организации VPN IPSec	Отчет по лабораторной работе
Самостоятельная работа	Проработка лекций	Экзамен
	Сетевые угрозы	Подготовка к экзамену
	Общие принципы защиты от сетевых атак	Подготовка к экзамену
	Защита сетевых устройств от несанкционированного доступа	Отчет по лабораторной работе и практическим занятиям
	Аутентификация, авторизация и учет	Отчет по лабораторной работе

	Защита сетей на канальном уровне	Отчет по лабораторной работе
	Защита сетей на основе списков контроля доступа	Отчет по лабораторной работе
	Виртуальные частные сети	Отчет по лабораторной работе
	Организация сетевой безопасности на межсетевых экранах	Подготовка к экзамну
	Защита оконечных устройств сетей	Отчет по практическим занятиям
	Подготовка к экзамену	Экзамен

4. Типовые контрольные задания

Представить один пример задания по каждому типу оценочных средств для каждой компетенции, формируемой данной дисциплиной.

ПК-1 – Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных

1. Задание на экзамен:

1.1 Понятие персональных данных. Места их хранения. Их важность для киберприступности.

1.2 Методы защиты межсетевых устройств от несанкционированного доступа. Требования, предъявляемые к паролям.

1.3 В Cisco Packet Tracer защитить консольный порт маршрутизатора от несанкционированного доступа. Доступ должен осуществляться с максимальными привилегиями. Обеспечить, что бы все пароли в маршрутизаторе были зашифрованы.

2. Задание на лабораторную работу №1 – 3:

2.1 Скоммутировать сеть, показанную на рисунке 1.

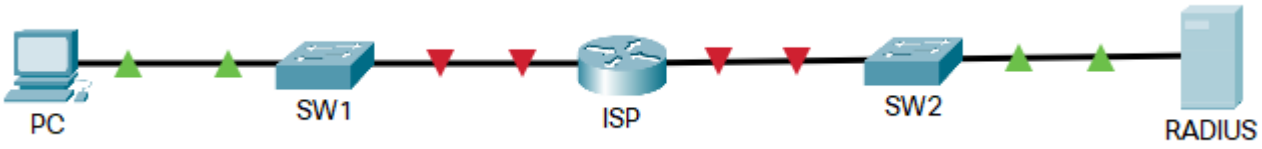

Рисунок 1 – Схема сети для настройки

По умолчанию на всех устройствах настроен удаленный доступ по протоколу Telnet.

2.2 На всех устройствах настроить сетевое имя, в соответствии со схемой на рисунке 1.

2.3 Настроить все межсетевые устройства так, что бы минимальная длина пароля была не менее пяти символов.

2.4 Настроить все межсетевые устройства так, что бы при двух не верно введенных паролей, в течение 1,5 минут, линия блокируется на одну минуту.

2.5 Настроить все межсетевые устройства так, что бы при бездействии в течении пяти минут, устройство завершало сеанс в привилегированном режиме.

2.6 Настроить все межсетевые устройства так, что бы все пароли хранились в зашифрованном виде.

2.7. Защитить консольные линии всех межсетевых устройств от несанкционированного доступа. **ВНИМАНИЕ!** Пароли должны быть надежными!

2.7.1 Коммутаторы с помощью пароля, который должен соответствовать вашему имени.

2.7.2 Маршрутизатор с помощью логина, который должен соответствовать вашим инициалам и паролем, который должен соответствовать вашей фамилии.

2.8 Защитить VTY всех межсетевых устройств от несанкционированного доступа. **ВНИМАНИЕ!** Пароли должны быть надежными!

2.8.1 Коммутаторы, используя модель AAA и локальную базу учетных записей. В качестве логина использовать вашу фамилию и инициалы, пароль придумать самостоятельно, который должен соответствовать всем требованиям к безопасности.

2.8.2 Доступ к маршрутизатору должен осуществляться с использованием RADIUS сервера. Логин для доступа root, пароль p@ssw0rd2022!. Ключевое слово

2.9 Защитить привилегированный режим всех межсетевых устройств от несанкционированного доступа. Пароль придумать самостоятельно, который должен соответствовать всем требованиям к безопасности. Пароль не должен совпадать с паролем в пункте 2.8.1. Пароль должен шифроваться 9 типом.

2.10 Ответить на контрольные вопросы.

3 Задание на практическое занятие 1 – 3.

3.1 Открыть файл ROMMON.

3.2 Ознакомиться с характеристикой корпоративной сети.

Компания состоит из двух офисов. Один находится в Екатеринбурге, другой в Первоуральске. В компании есть только то оборудование, которое показано на схеме. Другого нет.

ВНИМАНИЕ! Так как вы сотрудник офиса Первоуральска, то доступа к оборудованию Екатеринбурга у вас нет. Поэтому, ни каких действий совершать с оборудованием Екатеринбурга **НЕЛЬЗЯ!** Вы работаете исключительно с оборуждованием Первоуральска. Однако, условно можно позвонить в офис Екатеринбурга и узнать настройки ихнего оборудования. Это значит, что вы можете только посмотреть все необходимые настройки оборудования Екатеринбурга.

НЕЛЬЗЯ брать дополнительное обрудование и заменять существующее. По уловию запасного оборудрвания у вас нет. Все настройки необходимо выполнять исключительно с рабочего ноутбка Admin. Поэтому все скрины необхоимо сделать так, что бы было видно, что настройки ведутся с него.

3.3 Постановка проблемы.

В офисе Первоуральска была совершена внутренняя хакерская атака на оборудование. В результате вышло из строя оборудование. **НЕОБХОДИМО УЧЕСТЬ!** На маршрутизаторах должна стоять абсолютно одинаковая прошивка. Ваша задача: восстановить работу оборудования первого этажа в офисе Первоуральска так, что бы восстановить связь с офисом Екатеринбурга.

3.4 Требования к настройке.

3.4.1. На маршрутизаторе первого этажа необходимо выполнить следующие настройки:

1 Задать имя маршрутизатору в виде **вашей фамилии и инициалов**.

2 Задать доменное имя **Group<номер группы>.ru**. Вместо скобок указать свою группу.

3 Обеспечить доступ администратора из города Екатеринбурга к маршрутизатору по протоколу sshv2 с логином соответствующего **Вашему имени** и паролем **дата вашего рождния**. При успешной авторизации на маршрутизаторе, администратор должен ввести пароль **cisco** для доступа в привелигерованный режим.

4 Для связи с Екатеринбургом, нужна настройка, которую Вы не знаете, как выполнять. Однако, конфигурация с этой настройкой хранится на сервере tftp, под именем **Perv1.txt**.

5 Необходимо установить пароль на доступ к маршрутизатору по консольному порту. Логин для доступа **ваши инициалы**, пароль, **текущая дата**. При успешной авторизации на консольном порту, пользователь сразу должен попасть в привилегированный режим.

6 Все пароли должны хранится в зашифрованном виде.

3.4.2 На коммутаторе первого этажа были стерты все настройки. Они должны быть аналогичны настройкам коммутатора второго этажа. Необходимо восстановить эти настройки. После восстановления настроек обеспечить доступ администратору Екатеринбурга к коммутатору по защищенному соединению версии 2. Все коммутаторы должны взаимодествовать со своими маршрутизаторами, т. е. должен проходить пинг.

3.4.3 На маршрутизаторе второго этажа злоумышлинник изменил настройки и установил пароль на привилегированный режим. Необходимо:

1. Восстановить сетевое имя.

2. Обеспечить доступ администратору Екатеринбурга по защищенной удаленной связи с именем и паролем, аналогичным маршрутизатору Perv1.

3. Защитить привилегированный режим своим паролем.

4. Защитить доступ через консольный порт только по паролю **P@ssw0rd.**

3.4.4 Все устройства должны быть синхронизированы по времени.

3.5 Проверить, что бы все выполняемые задачи сети выполнялись.

3.6 Сделать резервные копии всех устройств Певоуральска.

4 Задание по самостоятельной работе

Оформить отчет по лабораторной работе №1-3 в соответствии с требованиями содержания:

4.1 Наименование работы.

4.2 Цель работы.

4.3 Состав оборудования.

4.4 Схема сети, в соответствии с рисунком 1.

4.5 Скриншоты подтверждающие выполнение настроек.

4.6 План IP-адресации сети.

4.7 Таблица с логинами и паролями для доступа к устройствам.

4.8 Ответы на контрольные вопросы.

ПК-8 - Способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных

1. Задание на экзамен:

1.1 Понятие корпоративных данных. Понятие их конфиденциальности, целостности и доступности. Последствия нарушения безопасности данных.

1.2 Методы защиты межсетевых устройств от несанкционированного доступа. Защита удаленного доступа. Сравнительная характеристика протоколов Telnet и ssh.

1.3 В Cisco Packet Tracer обеспечить удаленный защищенный доступ к маршрутизатору только по пяти vty линиям. Доступ должен осуществляться с минимальными привилегиями.

2. Задание на лабораторную работу №4-5:

2.1 Скоммутировать сеть, показанную на рисунке 1.

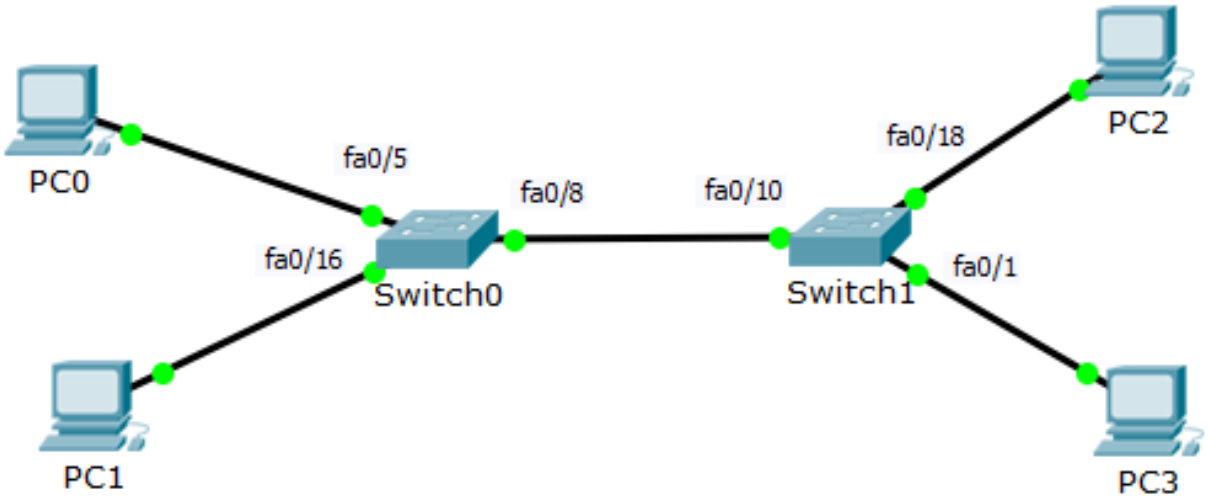

Рисунок 1 – Сеть для настройки

2.2 Через порт fa0/10 могли работать только PC0 и PC1. При нарушении режима безопасности должны формироваться сообщения в журнал логов, но порт отключаться не должен.

2.3 Через порт fa0/8 должны работать не более трех компьютеров, два из которых обязательно PC3 и PC4. При нарушении режима безопасности должен только блокироваться трафик.

2.4 Через порты fa0/1, 5, 16, 18 должны работать только соответствующие PC. При нарушении режима безопасности эти порты должны блокироваться.

2.5 Настроить порты fa0/5 и 16 так, что бы при отсутствии активности на этих портах в течение 5 минут, защита удалялась

2.6 Настроить порты fa0/1 и 18 так, что бы защита удалялась через 15 минут.

2.7 На Switch0 предусмотреть два порта через которые смогут подключиться к сети не более трех компьютеров.

2.8 На Switch1 предусмотреть три порта через которые смогут подключиться к сети не более двух компьютеров.

2.9 Все порты коммутаторов должны быть защищены от несанкционированного доступа.

2.10 Проверить правильность настройки коммутаторов.

3 Задание на практическое занятие

3.1 Открыть файл «Задание 1». PC1,2,5 в одном отделе PC4,6 в другом. PC одного отдела должны между собой взаимодействовать. Между отделами связи не должно быть. Проверить выполнение данного требования. Если не выполняется, то исправить ошибки в настройках Изменять подключения нельзя.

3.2 Открыть файл «Задание 2». PC должен иметь удаленный доступ к маршрутизатору по ssh. Изменять подключение нельзя. Пароль к консольному порту на маршрутизаторе 321. Проверить наличие доступа и исправить ошибки, если таковые есть.

3.3 Открыть файл «Задание 3». PC должен динамически получить IP-адрес. Менять настройки сервера и PC нельзя. Проверить получение IP-адреса и устранить неисправности, если такие есть.

3.4 Открыть файл «Задание 4». Через порт 10 должен работать только PC0. Но если к этому порту подключить PC2, то он тоже получает доступ к сети, т. е. пингуется PC3. Необходимо устранить данную проблему.

3.5 Открыть файл «Задание 5». Коммутатор SW4 был взломан и у него удалили конфигурационный файл. Настройки у него должны быть аналогичны коммутатору SW2. Выполните все необходимые настройки SW4, при этом, у вас очень ограничено время на восстановление коммутатора. Из-за простоя, компания теряет доходы.

3.6 Открыть файл «Задание 6». PC2 и PC3 должны между собой взаимодействовать. При этом, PC2 должен получать адрес по DHCP. PC0 должен взаимдействовать с PC1. Проверить выполнение этих условий и устранить неисправности, если таковые есть.

3.7 Открыть файл «Задание 7». В данной сети все компьютеры должны между собой взаимодействовать. Проверить наличие связи и устранить неисправности, если такие есть.

4 Задание по самостоятельной работе

Оформить отчет по лабораторной работе № 4-5 в соответствии с требованиями содержания:

4.1 Наименование работы.

4.2 Цель работы.

4.3 Схема сети и задание.

4.3 Скриншоты, подтверждающие настройки по разделу 5.

4.4 Ответы на контрольные вопросы.

5. Банк контрольных заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации

Представлен в электронной информационно-образовательной среде по URI: https://aup/uisi/ru

Оценочные средства рассмотрены и утверждены на заседании кафедры ИТиМС

28.05.2021 г Протокол № 9

Заведующий кафедрой (разработчика) _____ Н.В. Будылдина

подпись инициалы, фамилия

28.05.2021 г.

Оценочные средства рассмотрены и утверждены на заседании кафедры ИТиМС

28.05.2021 г Протокол № 9

Заведующий кафедрой (разработчика) _____ Н.В. Будылдина

подпись инициалы, фамилия

28.05.2021 г.