Федеральное агентство связи
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
«23» 12 2019 г.

РАБОЧАЯ ПРОГРАММА

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) – 2019

Екатеринбург 2019

Федеральное агентство связи
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
« ____» _____ 2019 г.

Р А Б О Ч А Я П Р О Г Р А М М А

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) – 2019

Екатеринбург 2019

Рабочая программа дисциплины «Защита информации от несанкционированного доступа» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» и Положением об организации и осуществления в СибГУТИ образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры.

Программу составил:

старший преподаватель		/ Е.С. Тарасов
должность	подпись	инициалы, фамилия
/ /		/
должность	подпись	инициалы, фамилия

Утверждена на заседании ОПДТС от 28.05.19 протокол № 8 кафедры

Заведующий кафедрой (разработчика) _____ / Н.В. Будылдина/
подпись инициалы, фамилия

28.05.19 г.

Заведующий кафедрой (выпускающей) _____ / Н.В. Будылдина/
подпись инициалы, фамилия

28.05.19 г.

Согласовано
Ответственный по ОПОП (руководитель ОПОП) _____ / Н.В. Будылдина /
подпись инициалы, фамилия

28.05.19 г.

Основная и дополнительная литература, указанная в рабочей программе, имеется в наличии в библиотеке института и ЭБС.

Зав. библиотекой _____ / С.Г.Торбенко
подпись инициалы, фамилия

Рабочая программа дисциплины «Защита информации от несанкционированного доступа» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 11.03.02 «Инфокоммуникационные технологии и системы связи» и Положением об организации и осуществления в СибГУТИ образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры.

Программу составил:

старший преподаватель		/ Е.С. Тарасов
должность	подпись	инициалы, фамилия
/ /		/
должность	подпись	инициалы, фамилия

Утверждена на заседании ОПДТС от 28.05.19 протокол № 8 кафедры

Заведующий кафедрой (разработчика) _____ / Н.В. Будылдина/
подпись инициалы, фамилия

28.05.19 г.

Заведующий кафедрой (выпускающей) _____ / Н.В. Будылдина/
подпись инициалы, фамилия

28.05.19 г.

Согласовано
Ответственный по ОПОП (руководитель ОПОП) _____ / Н.В. Будылдина /
подпись инициалы, фамилия

28.05.19 г.

Основная и дополнительная литература, указанная в рабочей программе, имеется в наличии в библиотеке института и ЭБС.

Зав. библиотекой _____ / С.Г.Торбенко
подпись инициалы, фамилия

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к вариативной части учебного плана. Шифр дисциплины в учебном плане – *Б1.В.24.*

ПК-1 – Способен к эксплуатации и развитию сетевых платформ, систем и сетей передачи данных	
Предшествующие дисциплины и практики	Основы теории цепей, ЭВМ и периферийные устройства, Вычислительная техника и информационные технологии, Элементная база телекоммуникационных систем, Языки программирования, Программирование сетевых приложений, Схемотехника телекоммуникационных устройств, Базы данных в телекоммуникациях, Теория связи, Сетевые технологии высокоскоростной передачи данных, Направляющие среды электросвязи, Операционные системы, Архитектура и программное обеспечение сетевых инфокоммуникационных устройств, Нормативно-правовая база профессиональной деятельности, Корпоративные инфокоммуникационные системы и услуги, Системы сетевого сопровождения инфокоммуникационных систем и услуг, Цифровые системы распределения сообщений, Пакетные радиосети, Сети и системы мобильной связи, Теория телетрафика, Проектирование и эксплуатация сетей связи, Электропитание устройств и систем телекоммуникаций
Дисциплины и практики, изучаемые одновременно с данной дисциплиной	Мультисервисные сети и протоколы, Экономика отрасли инфокоммуникаций, Планирование развития услуг связи на базе инфокоммуникационных систем.
Последующие дисциплины и практики	
ПК-8 - Способен осуществлять администрирование сетевых подсистем инфокоммуникационных систем и/или их составляющих	
Предшествующие дисциплины и практики	Программирование сетевых приложений, Схемотехника телекоммуникационных устройств, Базы данных в телекоммуникациях, Теория связи, Сетевые технологии высокоскоростной передачи данных, Направляющие среды электросвязи, Операционные системы, Архитектура и программное обеспечение сетевых инфокоммуникационных устройств, Нормативно-правовая база профессиональной деятельности, Корпоративные инфокоммуникационные системы и услуги, Системы сетевого сопровождения инфокоммуникационных систем и услуг, Пакетные радиосети, Сети и системы мобильной связи.
Дисциплины и практики, изучаемые одновременно с данной дисциплиной	Мультисервисные сети и протоколы.
Последующие дисциплины и практики	

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины обучающийся должен демонстрировать освоение следующих компетенций по дескрипторам «знания, умения, владения», соответствующие тематическим разделам дисциплины, и применимые в их последующем обучении и профессиональной деятельности:

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

Знать
- виды сетевых угроз и методы их реализации;
- методы криптографичекой защиты информации;
- методы защиты от сетевых угроз на разных уровнях эталонной модели;
- методы организации виртуальных частных сетей;
- методы защиты информации на оконечном оборудовании.

Уметь
- настраивать функцию Port Security;
- создавать Access Control List;
- настраивать функции брандмауэра;
- защищать сетевое оборудование от несанкционированного доступа;
- создавать VPN соединения

Владеть
- навыками решения производственных задач по защите сетевой безопасности.

ПК-8 - Способен осуществлять администрирование сетевых подсистем инфокоммуникационных систем и/или их составляющих

Знать
- виды сетевых угроз и методы их реализации;
- методы криптографичекой защиты информации;
- методы защиты от сетевых угроз на разных уровнях эталонной модели;
- методы организации виртуальных частных сетей;
- методы защиты информации на оконечном оборудовании.

Уметь
- настраивать функцию Port Security;
- создавать Access Control List;
- настраивать функции брандмауэра;
- защищать сетевое оборудование от несанкционированного доступа;
- создавать VPN соединения

Владеть
- навыками решения производственных задач по защите сетевой безопасности.

3. ОБЪЁМ ДИСЦИПЛИНЫ

3.1 Очная форма обучения

Общая трудоемкость дисциплины, изучаемой в _8_ семестре, составляет _3_ зачетных единиц. По дисциплине предусмотрен экзамен.

Виды учебной работы	Всего часов/зачетных единиц	Семестр
		8
Аудиторная работа (всего)	**64/1,77**	**64**
В том числе в интерактивной форме	**16/0,44**	**16**
Лекции (ЛК)	18/0,5	18
Лабораторные работы (ЛР)	34/0,94	34
Практические занятия (ПЗ)	10/0,27	10
Промежуточный контроль (ПР)	2/0,05	2
Самостоятельная работа студентов (всего)	**26/0,72**	**26**
Проработка лекций	6/0,16	6
Подготовка к практическим занятиям и оформление отчетов	4/0,11	4
Подготовка к лабораторным занятиям и оформление отчетов	10/0,27	10
Выполнение курсовой работы		
Выполнение РГР**	-	-
Подготовка и сдача экзамена**	6/0,16	6
Контроль	**18/0,5**	**18**
Общая трудоемкость дисциплины, **часов**	**108/3**	**108/3**

Одна зачетная единица (ЗЕ) эквивалентна 36 часам.

**** Оставить нужное**

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ

4.1 Содержание лекционных занятий

№ раздела дисциплины	Наименование лекционных тем (разделов) дисциплины и их содержание	Объем в часах		
		О	З	$З_д$
1	**Сетевые угрозы** Основные причины необходимости защиты информации и данных. Общие принципы защиты информации в различных сетях. Основные понятия угроз безопасности: угроза, уязвимость, риск, хакер. Виды хакеров и их особенности. Основные инструменты проникновения в сеть. Их задачи. Вредоносные программы, их особенности и принцип работы. Типы сетевых атак, их характеристики и принцип реализации.	2		
2	**Общие принципы защиты от сетевых атак** Политика сетевой безопасности. Средства тестирования сетевой безопасности, их назначение. Методы смягчения последствий распространенных сетевых атак.	2		
3	**Защита сетевых устройств от несанкционированного доступа** Методы административного доступа к межсетевым устройствам: локальный и удаленный. Их особенности и область использования. Протоколы удаленного доступа: Telnet и SSH. Их сравнительная характеристика. Требования к паролям для обеспечения их надежности. Алгоритмы хэширования паролей. Защита паролей от подбора. Настройка повышенной безопасности локального и удаленного доступа к устройствам.	2		
4	**Аутентификация, авторизация и учет** Понятие аутентификации, авторизации и учета. Виды аутентификации: локальная и на основе сервера. Их сравнительная характеристика. Протокол серверной аутентификации RADIUS. Его характеристика. Процедурные характеристики. Принципы организации серверной авторизации и учета.	2		
5	**Защита сетей на канальном уровне** Виды атак на канальном уровне ЭМ ВОС: атаки на таблицы MAC, VLAN, DHCP, ARP, STP, адресные атаки с подменой. Механизмы их реализации. Использование функции Port Security. Методы ограничения количества распознаваемых адресов. Режимы нарушения безопасности. Защита от атак на VLAN, DHCP, ARP, STP, адресные атаки с подменой.	2		
6	**Защита сетей на основе списков контроля доступа** Понятие списков контроля доступа (ACL). Их задачи. Виды списков и их особенности. Общий принцип работы. Понятие шаблонной маски. Виды шаблонных масок и методика ее вычисления. Методики создания стандартных и расширенных списков контроля доступа. Методы изменения ACL. Использование ACL для защиты от атак ICMP и SNMP. Использование списков контроля доступа для IPv6. Настройка разнотипных списков контроля доступа. Понятие NAT. Назначение. Виды NAT и принцип их реализации. Настройка разнотипного NAT. Сравнительная характеристика NAT и PAT. Особенности применения PAT. Его настройка.	2		

7	**Виртуальные частные сети** Понятие виртуальных частных сетей (VPN). Преимущества их использования. Методы построения VPN: с удаленным доступом, SSL, IPSec. Их особенности. Основные функции безопасности протокола IPSec. Протоколы IPSec: AH, ESP, IKE. Форматы протоколов и принцип их работы. Принцип настройки VPN IPSec.	2		
8	**Организация сетевой безопасности на межсетевых экранах** Назначение межсетевого экрана. Виды межсетевых экранов и их особенности, достоинства и недостатки. Место межсетевых экранов в организации многоуровневой системы сетевой безопасности. Архитектуры безопасности на межсетевых экранах: частные и государственные, демилитаризованные зоны (DMZ), на основе зон (ZPF). Преимущества использования ZPF. Этапы их создания. Настройка ZPF на межсетевых экранах. Настройка различных функций сетевой защиты на межсетевых экранах.	2		
9	**Защита оконечных устройств сетей** Основные сетевые угрозы для оконечного оборудования. Методы атаки на него. Основные признаки наличия различных атак на оборудование. Методы защиты оконечного оборудования от сетевых атак. Защита сети от несанкционированного доступа по протоколу IEEE 802.1X. Роли устройств при аутентификации. Процедурная характеристика протокола. Настройка аутентификации по проколу IEEE 802.1X	2		
	ВСЕГО	**18**		

4.2 Содержание практических занятий

№ п/п	№ раздела дисциплины	Наименование лабораторных работ, практических занятий	Объем в часах		
			О	З	$З_Д$
1	3	Изучение принципов управления конфигурацией и образами IOS	6		
2	8	Поиск и устранение неисправностей в обеспечении безопасности сетей передачи данных	4		
		ВСЕГО	**10**		

4.3 Содержание лабораторных занятий

№ п/п	№ раздела дисциплины	Наименование лабораторных работ, практических занятий	Объем в часах		
			О	З	$З_Д$
1	4	Исследование методов защиты сетевых устройств от несанкционированного доступа	6		
2	5	Настройка сетевой безопасности с помощью функции Port Security	4		
3	5	Исследование принципов организации защиты сетей с использованием VLAN	6		
	6	Исследование принципов настройки стандартных ACL	6		
5	7	Исследование принципов настройки службы NAT	6		
4	7	Исследование принципов организации VPN IPSec	6		
		ВСЕГО	**34**		

5. ПЕРЕЧЕНЬ ИННОВАЦИОННЫХ ФОРМ УЧЕБНЫХ ЗАНЯТИЙ[1]

Преподавание дисциплины базируется на результатах научных исследований, проводимых УрТИСИ СибГУТИ, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей.

№ п/п	Тема	Объем в часах*		Вид учебных занятий	Используемые инновационные формы занятий
		О	З		
1	Общие принципы защиты от сетевых атак	2	2	Лекция	Групповые дискуссии
2	Изучение принципов безопасного управления устройствами	2		Практическое занятие	Обсуждение проблем прикладного характера
3	Исследование методов защиты сетевых устройств от несанкционированного доступа	6		Лабораторная работа	Мастер-класс
4	Исследование принципов настройки службы NAT	6		Лабораторная работа	Мастер-класс
	ВСЕГО	**16**	**2**		

* Не меньше интерактивных часов

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПО ДИСЦИПЛИНЕ

6.1 Список основной литературы

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]:/ Шаньгин В. Ф.-Электрон. Текстовые данные.-Саратов: Профобразование, 2017.- 544 c. - Режим доступа: http://www.iprbookshop.ru/63592.html.

2. Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П. Н., Бабаш А. В., Баранова Е. К.- Электрон. Текстовые данные.- М.: Евразийский открытый институт, 2012.- 311 c. Режим доступа: http://www.iprbookshop.ru/10677.html.

6.2 Список дополнительной литературы

1. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н. А. Свинарев [и др.].- Электрон. Текстовые данные.- Воронеж: Воронежский государственный университет инженерных технологий, 2013.- 192 c.— Режим доступа: http://www.iprbookshop.ru/47422.html.

6.3 Информационное обеспечение (в т.ч. интернет- ресурсы).

1. Официальный сайт UISI.RU/ (дата обращения: 15.05.2019)
2. Единая научно-образовательная электронная среда (Е-НОЭС) УрТИСИ http://aup.uisi.ru/

[1] Учесть развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей).

3. Электронная библиотечная система «IPRbooks» /http://www.iprbookshop.ru/ доступ по логину и паролю

4. Электронный каталог АБК ASBOOK

5. Полнотекстовая база данных учебных и методических пособий СибГУТИ http://ellib.sibsutis.ru/cgi-bin/irbis64r_12/cgiirbis_64.exe?LNG= &C21COM=F&I21DBN=ELLIB&P21DBN=ELLIB&S21FMT=&S21ALL=&Z21ID=&S21CNR= доступ по логину и паролю

6. Научная электронная библиотека (НЭБ) elibrary http://www.elibrary.ru

7. Единое окно доступа к образовательным ресурсам http://window.edu.ru/

8. Сетевая академия Cisco. Курс «Network Security» https://www.netacad.com

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ И ТРЕБУЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Наименование аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Лекционная аудитория	Лекционные занятия	– компьютер; – мультимедийный проектор; – экран; – доска.
Лаборатория 205 УК№3	Лабораторные и практические работы	- персональные компьютеры подключенные в локальную сеть и сеть Интернет, работающие под управлением операционной системы Windows Server 2016 и Windows 10, - коммутатор Cisco 2960, - маршрутизатор Cisco 2901, 2800, - межсетевой экран ASA 5505, - программное обеспечение OpenOffice, - программный пакет Cisco Packet Tracer.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ[2]

8.1 Подготовка к лекционным, практическим и лабораторным занятиям

На лекциях необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание научных явлений и процессов, научные выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты в соответствии с вопросами плана лекции, предложенными преподавателем. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале.

Во время лекции можно задавать преподавателю уточняющие вопросы с целью освоения теоретических положений, разрешения спорных вопросов.

8.2 Самостоятельная работа студентов

Успешное освоение компетенций, формируемых данной учебной дисциплиной, предполагает оптимальное использование времени самостоятельной работы.

[2] Целью методических указаний является обеспечение обучающимся оптимальной организации процесса изучения дисциплины.

Подготовка к лекционным занятиям включает выполнение всех видов заданий, рекомендованных к каждой лекции, т. е. задания выполняются еще до лекционного занятия по соответствующей теме. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Все задания к лабораторным работам, а также задания, вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующей темы лекционного курса, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «пробелы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к получению новых знаний и овладению навыками.

Самостоятельная работа во внеаудиторное время состоит из:

- повторения лекционного материала;
- подготовки лабораторным работам;
- подготовка к практическим занятиям;
- изучения учебно-методической и научной литературы;
- изучения нормативно-правовых актов;
- решения задач, предусмотренных на лабораторных работах;
- подготовки к контрольным работам, тестированию и т. д.;
- подготовки к семинарам устных докладов (сообщений);
- выполнения контрольных работ по заданию преподавателя;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах дисциплины задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы.

8.3 Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации необходимо:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендуемую литературу;
- составить краткие конспекты ответов (планы ответов).

Освоение дисциплины предусматривает посещение лекционных занятий, выполнение и защиту лабораторных, практических работ, самостоятельной работы.

Текущий контроль достижения результатов обучения по дисциплине включает следующие процедуры:

-контрольные работы для полусеместровой аттестации;

-контроль самостоятельной работы, осуществляемый на каждом практическом занятии и и лабораторной, работе;

-защита лабораторных работ.

Промежуточный контроль достижения результатов обучения по дисциплине проводится в следующих формах:

- экзамен (8 семестр).

Для проведения текущего контроля и промежуточной аттестации используются оценочные средства, описание которых расположено в Приложении 1 и на сайте (http://www.aup.uisi.ru).