Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный индустриальный университет»

Кафедра прикладных информационных технологий и программирования

УТВЕРЖДАЮ
Директор института
информационных технологий и
автоматизированных систем
_____ Л.Д. Павлова
подпись
«____» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность компьютерных сетей

09.02.06 «Сетевое и системное администрирование»

Квалификация выпускника
Сетевой и системный администратор

Форма обучения
Очная форма

Срок обучения: 3 года 10 месяцев

Год начала подготовки 2023

Новокузнецк
2023

СибГИУ
Подлинник электронного документа хранится в системе электронного согласования документов СибГИУ
ДОКУМЕНТ ПОДПИСАН ЭП
Сертификат: 861a8d56fc2cfb6de53bd665403c592fd02b1419
Владелец: Ректор Юрьев Алексей Борисович
Действителен: с 12 февраля 2024 г. по 7 мая 2025 г.
Дата и время: 01-03-2024 01:55:55 ПРОВЕРИТЬ ПОДПИСЬ

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний и умений по защите компьютерных сетей с применением программно-аппаратных средств;
– понимание основных принципов, технологий и архитектур проектирования и реализации операционных систем.

Задачами учебной дисциплины являются:

– систематическое изложение лекционного материала по безопасности компьютерных сетей;
– формирование знаний о методах и средствах защиты информации в компьютерных сетях;
– формирование знаний о методах и средствах построения виртуальных частных сетей;
– формирование знаний о методах и средствах аудита уровня защищенности информационных систем.

2 Место учебной дисциплины в структуре ООП по специальности

Учебная дисциплина входит в состав профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» профессионального цикла ООП по специальности 09.02.06 «Сетевое и системное администрирование».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Компьютерные сети;
– Организация, принципы построения и функционирования компьютерных сетей;
– Информационные технологии.

Учебная дисциплина дополняет умения и знания, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Администрирование сетевых операционных систем.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции

– ПК 3.1.: Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
– ПК 3.2.: Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

– ПК 3.3.: Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.

– ПК 3.4.: Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

– ПК 3.5.: Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

– ПК 3.6.: Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Обучающийся должен быть готов к выполнению основных видов профессиональной деятельности:

– выполнение работы по проектированию сетевой инфраструктуры;
– организация сетевого администрирования;
– эксплуатация объектов сетевой инфраструктуры.

В результате освоения учебной дисциплины обучающийся должен уметь, знать, иметь практический опыт:

Код ОК, ПК	**Уметь**	**Знать**	**Иметь практический опыт**
ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ПК 3.6.	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; осуществлять диагностику и поиск неисправностей всех компонентов сети; выполнять действия по устранению неисправностей	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа локальных сетей; методы устранения неисправностей в технических средствах	в обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя; в удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры; в поддержке пользователей сети, в настройке аппаратного и программного обеспечения сетевой инфраструктуры

4 Объем и содержание учебной дисциплины

Учебная деятельность обучающихся предусматривает учебные занятия (лекция, практическое занятие, консультация), самостоятельную работу, а также другие виды учебной деятельности, определенные учебным планом и календарным планом воспитательной работы.

Объем учебной дисциплины

Семестр / курс	***ИТОГО***	***6 семестр***	***7 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость, *академ. час.*	***145***	*48*	*97*
Лекции, *академ. час.*	***32***	*16*	*16*
в форме практической подготовки	***0***	*0*	*0*
Лабораторные работы, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Практические занятия, *академ. час.*	***48***	*16*	*32*
в форме практической подготовки	***0***	*0*	*0*
Курсовая работа / проект, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Консультации, *академ. час.*	***1***	*0*	*1*
в форме практической подготовки	***0***	*0*	*0*
Самостоятельная работа, *академ. час.*	***58***	*16*	*42*
в форме практической подготовки	***0***	*0*	*0*
Контроль, *академ. час.*	***6***	*0*	*6*
в форме практической	***0***	*0*	*0*

подготовки			

Содержание учебной дисциплины

Раздел 1 Фундаментальные принципы безопасной сети (Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.);

Раздел 2 Безопасность Сетевых устройств OSI (Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.);

Раздел 3 Авторизация, аутентификация и учет доступа (AAA) (Свойства AAA. Локальная AAA аутентификация. Server-based AAA.);

Раздел 4 Реализация технологий брандмауэра (ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах.);

Раздел 5 Реализация технологий предотвращения вторжения (IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS.);

Раздел 6 Безопасность локальной сети (Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей.);

Раздел 7 Криптографические системы (Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.);

Раздел 8 Реализация технологий VPN (VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN. Реализация Site-to-site IPSec VPN.);

Раздел 9 Управление безопасной сетью (Принципы безопасности. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Разработка регламентов компании и политик безопасности.);

Раздел 10 Понятие о методах и средствах аудита уровня защищенности информационных систем (Введение в технический анализ всех элементов компьютерной сети. Выявление проблем функционирования сети и составление рекомендаций по их устранению. Оценка качества, инвентаризация и документирование.).

5 Перечень тем лекций

№ раздела / темы дисциплины	**Темы лекций**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**

Раздел 1.	Фундаментальные принципы безопасной сети	3	
Раздел 2.	Безопасность Сетевых устройств OSI	3	
Раздел 3.	Авторизация, аутентификация и учет доступа (AAA)	3	
Раздел 4.	Реализация технологий брандмауэра	3	
Раздел 5.	Реализация технологий предотвращения вторжения	3	
Раздел 6.	Безопасность локальной сети	3	
Раздел 7.	Криптографические системы	3	
Раздел 8.	Реализация технологий VPN	3	
Раздел 9.	Управление безопасной сетью	4	
Раздел 10.	Введение в аудит элементов компьютерной сети	4	
Итого:		**32**	**0**

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	**Темы практических занятий (семинаров)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 2.	Настройка безопасного доступа к маршрутизатору	4	
Раздел 3.	Обеспечение административного доступа AAA и сервера	5	
Раздел 4.	Настройка политики безопасности брандмауэров	5	
Раздел 5.	Начальная настройка системы предотвращения вторжений (IPS)	5	
Раздел 6.	Исследование сетевых атак и инструментов проверки защиты сети.	5	
Раздел 7.	Криптографические системы	5	
Раздел 8.	Практическая настройка сервиса VPN	5	
Раздел 9.	Аудит безопасности. Получение информации из открытых источников	5	

Раздел 9.	Аудит безопасности. Получение информации от сетевых сервисов	6	
Раздел 10.	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	3	
Итого:		**48**	**0**

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	**Темы лабораторных работ**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	**Темы курсовых работ (проектов)**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
	Отсутствуют		
Итого:		**0**	**0**

9 Виды самостоятельной работы

№ раздела / темы дисциплины	**Виды самостоятельной работы**	**Трудоемкость, *академ.час***	
		всего	**в форме практической подготовки**
Раздел 1.	1. Изучение лекционного материала; 2. Прохождение тестирования.	5	
Раздел 2.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 3.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к	6	

	практическому занятию; 4. Прохождение тестирования.		
Раздел 4.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 5.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 6.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 7.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 8.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 9.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
Раздел 10.	1. Изучение лекционного	5	

	материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.		
	Консультации	1	
Контроль	*Подготовка к экзамену*	6	
Итого:		**65**	**0**

10 Учебно-методическое и информационное обеспечение учебной дисциплины

а) основная литература:

1 Новожилов, О. П. Информатика : учебник для среднего профессионального образования. В 2 ч. Часть 1 / О. П. Новожилов. – 3-е изд., пер. и доп. – Москва : Юрайт, 2022. – 320 с. – ISBN 978-5-534-06372-1. – URL: https://urait.ru/bcode/493964 (дата обращения: 15.05.2023);

2 Новожилов, О. П. Информатика : учебник для среднего профессионального образования. В 2 ч. Часть 2 / О. П. Новожилов. – 3-е изд., пер. и доп. – Москва : Юрайт, 2022. – 302 с. – ISBN 978-5-534-06374-5. – URL: https://urait.ru/bcode/493965 (дата обращения: 15.05.2023);

3 Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., пер. и доп. – Москва : Издательство Юрайт, 2022. – 161 с. – ISBN 978-5-534-13948-8. – URL: https://urait.ru/bcode/495525 (дата обращения: 15.05.2023).

б) дополнительная литература:

1 Новожилов, О. П. Архитектура компьютерных систем : учебное пособие для среднего профессионального образования. В 2 ч. Часть 1 / О. П. Новожилов. – Москва : Издательство Юрайт, 2022. – 276 с. – ISBN 978-5-534-10299-4. – URL: https://urait.ru/bcode/495226 (дата обращения: 15.05.2023);

2 Новожилов, О. П. Архитектура компьютерных систем : учебное пособие для среднего профессионального образования. В 2 ч. Часть 2 / О. П. Новожилов. – Москва : Издательство Юрайт, 2022. – 246 с. – ISBN 978-5-534-10301-4. – URL: https://urait.ru/bcode/495227 (дата обращения: 15.05.2023);

в) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». – Москва, [200 –]. – URL:

http://www.studentlibrary.ru. – Режим доступа: для авторизир. пользователей;

2 ЛАНЬ : электронно-библиотечная система : [коллекция «Инженерно-технические науки»] / ООО «Издательство ЛАНЬ». – Санкт-Петербург, [200 –]. – URL: http://e.lanbook.com. – Режим доступа: для авторизир. пользователей;

3 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». – Москва, [200 –]. – URL: http://elibrary.ru. – Режим доступа: по подписке;

4 Национальная электронная библиотека (НЭБ) : информационная система / ФГБУ «РГБ». – Москва, [2015 –]. – URL: http://rusneb.ru. – Режим доступа: по подписке;

5 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». – Москва, [200 –]. – URL: https://urait.ru. – Режим доступа: для авторизир. пользователей;

6 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». – Москва, [200 –]. – URL: https://biblioclub.ru. – Режим доступа: для авторизир. пользователей. – URL: http://www.biblioclub.ru;

7 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. – Новокузнецк, [200 –]. – URL: http://library.sibsiu.ru/LibrELibraryFullText.asp. – Режим доступа: для авторизир. пользователей. – URL: https://library.sibsiu.ru/LibrELibraryFullText.asp;

8 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». – Москва, [200 –]. – URL: http://eivis.ru. – Режим доступа: по подписке;

9 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: http://libr.sibsiu.ru. – URL: https://libr.sibsiu.ru.

г) лицензионное и свободно распространяемое программное обеспечение:

– VirtualBox.

д) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

11 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории для проведения занятий всех видов, предусмотренных учебным планом, в том числе для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, кабинеты, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов.
Для проведения занятий лекционного типа (лекций) предусмотрена аудитория, оборудованная компьютерной техникой, экраном и мультимедийным проектором, учебной доской? для проведения практических занятий предусмотрены лаборатории «Организация и принципы построения компьютерных систем», оснащенные 12-15 компьютерами обучающихся и 1 компьютером преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ, пакет САПР), сервером в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение: Windows Server 2012 или более новая версия, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионный программы по виртуализации.), компьютерами с лицензионным программным обеспечением, интерактивной доской, 6 маршрутизаторами, 6 коммутаторами, телекоммуникационной стойкой, 2 беспроводными маршрутизаторами Linksys, IP телефонами 3 шт., программно-аппаратными шлюзами безопасности 2 шт., 1 компьютером для лабораторных занятий с ОС Microsoft Windows Server, Linux и системами виртуализации.
Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС СПО по направлению подготовки (специальности) 09.02.06 «Сетевое и системное администрирование».

Составитель(и):

преподаватель Грачев Александр Викторович (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Приложение

Аннотация
рабочей программы дисциплины «Безопасность компьютерных сетей»

по направлению подготовки (специальности)
09.02.06 «Сетевое и системное администрирование»
форма обучения – Очная форма

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

– формирование у обучающихся знаний и умений по защите компьютерных сетей с применением программно-аппаратных средств;
– понимание основных принципов, технологий и архитектур проектирования и реализации операционных систем.

Задачами учебной дисциплины являются:

– систематическое изложение лекционного материала по безопасности компьютерных сетей;
– формирование знаний о методах и средствах защиты информации в компьютерных сетях;
– формирование знаний о методах и средствах построения виртуальных частных сетей;
– формирование знаний о методах и средствах аудита уровня защищенности информационных систем.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина входит в состав профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» профессионального цикла ООП по специальности 09.02.06 «Сетевое и системное администрирование».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

– Компьютерные сети;
– Организация, принципы построения и функционирования компьютерных сетей;
– Информационные технологии.

Учебная дисциплина дополняет умения и знания, получаемые по одновременно изучаемым и последующим учебным дисциплинам:

– Администрирование сетевых операционных систем.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции

– ПК 3.1.: Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

– ПК 3.2.: Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

– ПК 3.3.: Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.

– ПК 3.4.: Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

– ПК 3.5.: Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

– ПК 3.6.: Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Обучающийся должен быть готов к выполнению основных видов профессиональной деятельности:

– выполнение работы по проектированию сетевой инфраструктуры;
– организация сетевого администрирования;
– эксплуатация объектов сетевой инфраструктуры.

В результате освоения учебной дисциплины обучающийся должен уметь, знать, иметь практический опыт:

Код ОК, ПК	**Уметь**	**Знать**	**Иметь практический опыт**
ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5. ПК 3.6.	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; осуществлять диагностику и поиск неисправностей всех компонентов сети; выполнять действия по устранению неисправностей	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа локальных сетей; методы устранения неисправностей в технических	в обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя; в удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры; в поддержке пользователей сети, в настройке аппаратного и программного

		средствах	обеспечения сетевой инфраструктуры

4 Объем учебной дисциплины

Семестр / курс	***ИТОГО***	***6 семестр***	***7 семестр***
Форма промежуточной аттестации			*экзамен*
Трудоёмкость, *академ. час.*	***145***	*48*	*97*
Лекции, *академ. час.*	***32***	*16*	*16*
в форме практической подготовки	***0***	*0*	*0*
Лабораторные работы, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Практические занятия, *академ. час.*	***48***	*16*	*32*
в форме практической подготовки	***0***	*0*	*0*
Курсовая работа / проект, *академ. час.*	***0***	*0*	*0*
в форме практической подготовки	***0***	*0*	*0*
Консультации, *академ. час.*	***1***	*0*	*1*
в форме практической подготовки	***0***	*0*	*0*
Самостоятельная работа, *академ. час.*	***58***	*16*	*42*
в форме практической подготовки	***0***	*0*	*0*
Контроль, *академ. час.*	***6***	*0*	*6*
в форме практической подготовки	***0***	*0*	*0*

5 Краткое содержание учебной дисциплины

В структуре учебной дисциплины выделяются следующие основные разделы (темы):

Раздел 1 Фундаментальные принципы безопасной сети (Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.);

Раздел 2 Безопасность Сетевых устройств OSI (Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.);

Раздел 3 Авторизация, аутентификация и учет доступа (AAA) (Свойства AAA. Локальная AAA аутентификация. Server-based AAA.);

Раздел 4 Реализация технологий брандмауэра (ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах.);

Раздел 5 Реализация технологий предотвращения вторжения (IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS.);

Раздел 6 Безопасность локальной сети (Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей.);

Раздел 7 Криптографические системы (Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.);

Раздел 8 Реализация технологий VPN (VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN. Реализация Site-to-site IPSec VPN.);

Раздел 9 Управление безопасной сетью (Принципы безопасности. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Разработка регламентов компании и политик безопасности.);

Раздел 10 Понятие о методах и средствах аудита уровня защищенности информационных систем (Введение в технический анализ всех элементов компьютерной сети. Выявление проблем функционирования сети и составление рекомендаций по их устранению. Оценка качества, инвентаризация и документирование.).

6 Составитель(и):

преподаватель Грачев Александр Викторович (кафедра прикладных информационных технологий и программирования).