

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»

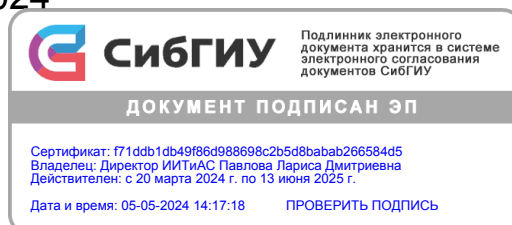
Квалификация выпускника
Системный администратор

Форма обучения
Очная форма

Срок обучения: 3 года 10 месяцев

Год начала подготовки 2024

Новокузнецк
2024



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 (по выбору)» 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:

Общие компетенции

- ОК 04.: Эффективно взаимодействовать и работать в коллективе и команде
- ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

– ОК 06.: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

Профессиональные компетенции

– ПК 3.1.: Осуществлять проектирование сетевой инфраструктуры.

– ПК 3.2.: Обслуживать сетевые конфигурации программно-аппаратных средств.

– ПК 3.3.: Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

– ПК 3.4.: Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.

– ПК 3.5.: Модернизировать сетевые устройства информационно-коммуникационных систем.

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
ОК 04. ОК 05. ОК 06. ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5.	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			<i>экзамен</i>
Трудоёмкость, <i>академ. час.</i>	168	48	120
Лекции, <i>академ. час.</i>	46	14	32
в форме практической подготовки	0	0	0
Лабораторные работы, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Практические занятия, <i>академ. час.</i>	64	16	48
в форме практической подготовки	0	0	0
Курсовая работа / проект, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Консультации, <i>академ. час.</i>	1	0	1
в форме практической подготовки	0	0	0
Самостоятельная работа, <i>академ. час.</i>	51	18	33
в форме практической подготовки	0	0	0

Контроль, <i>академ. час.</i>	6	<i>0</i>	6
в форме практической подготовки	0	<i>0</i>	0

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, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	Фундаментальные принципы безопасной сети	4	
Раздел 2.	Безопасность Сетевых устройств OSI	5	
Раздел 3.	Авторизация, аутентификация и учет доступа (AAA)	4	
Раздел 4.	Реализация технологий брандмауэра	4	
Раздел 5.	Реализация технологий предотвращения вторжения	4	
Раздел 6.	Безопасность локальной сети	5	
Раздел 7.	Криптографические системы	4	
Раздел 8.	Реализация технологий VPN	5	
Раздел 9.	Управление безопасной сетью	5	
Раздел 10.	Введение в аудит элементов компьютерной сети	6	
Итого:		46	0

6 Перечень тем практических занятий (семинаров)

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

	сервиса VPN		
Раздел 9.	Аудит безопасности. Получение информации из открытых источников	8	
Раздел 9.	Аудит безопасности. Получение информации от сетевых сервисов	8	
Раздел 10.	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	4	
Итого:		64	0

7 Перечень тем лабораторных работ

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

8 Перечень тем курсовых работ (проектов)

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

9 Виды самостоятельной работы

№ раздела / темы дисциплины	Виды самостоятельной работы	Трудоемкость, <i>академ. час</i>	
		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.	5	
Раздел 3.	1. Изучение лекционного	5	

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

	практическому занятию; 4. Прохождение тестирования.		
Раздел 10.	1. Изучение лекционного материала; 2. Оформление отчета о практической работе; 3. Подготовка к практическому занятию; 4. Прохождение тестирования.	6	
	<i>Консультации</i>	1	
<i>Контроль</i>	<i>Подготовка к экзамену</i>	6	
Итого:		58	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: 18.04.2024);

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: 18.04.2024);

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: 18.04.2024).

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: 18.04.2024);

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: 18.04.2024);

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

5 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>;

6 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>;

7 Электронная библиотека УМЦ ЖДТ : [коллекция «Эксплуатация железных дорог»] / ФГБУ ДПО «Учебно-методический центр по образованию на железнодорожном транспорте». – Москва, [2013 –]. – URL: <https://umczdt.ru/books/>. – Режим доступа: для авторизир. пользователей;

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:

- 7-Zip;
- Adobe Acrobat Reader;
- Astra Linux Special Edition;
- Kaspersky Endpoint Security;
- Microsoft Office;
- Microsoft Windows;
- OnlyOffice;

- VirtualBox;
- P7-Офис.

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).

Не задана информация о рассмотрении и утверждении.

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 (по выбору)» 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:

Общие компетенции

– ОК 04.: Эффективно взаимодействовать и работать в коллективе и команде

– ОК 05.: Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

– ОК 06.: Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

Профессиональные компетенции

– ПК 3.1.: Осуществлять проектирование сетевой инфраструктуры.

– ПК 3.2.: Обслуживать сетевые конфигурации программно-аппаратных средств.

– ПК 3.3.: Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

– ПК 3.4.: Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.

– ПК 3.5.: Модернизировать сетевые устройства информационно-коммуникационных систем.

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
ОК 04. ОК 05. ОК 06. ПК 3.1. ПК 3.2. ПК 3.3. ПК 3.4. ПК 3.5.	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; осуществлять диагностику и поиск неисправностей всех компонентов сети; выполнять действия	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа	в обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя; в удаленном администрировании и восстановлении работоспособности сетевой

	по устранению неисправностей	локальных сетей; методы устранения неисправностей в технических средствах	инфраструктуры; в поддержке пользователей сети, в настройке аппаратного и программного обеспечения сетевой инфраструктуры
--	------------------------------	--	--

4 Объем учебной дисциплины

Семестр / курс		6 семестр	7 семестр
Форма промежуточной аттестации	ИТОГО		<i>экзамен</i>
Трудоёмкость, <i>академ. час.</i>	168	48	120
Лекции, <i>академ. час.</i>	46	14	32
в форме практической подготовки	0	0	0
Лабораторные работы, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Практические занятия, <i>академ. час.</i>	64	16	48
в форме практической подготовки	0	0	0
Курсовая работа / проект, <i>академ. час.</i>	0	0	0
в форме практической подготовки	0	0	0
Консультации, <i>академ. час.</i>	1	0	1
в форме практической подготовки	0	0	0
Самостоятельная работа, <i>академ. час.</i>	51	18	33
в форме практической	0	0	0

подготовки			
Контроль, <i>академ. час.</i>	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).