Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное
учреждение высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Проректор по образовательной деятельности
_____ А.В. Зайцев
«28» сентября 2018 г.

Рабочая программа учебной дисциплины

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ

образовательной программы высшего образования –
программы специалитета
10.05.03 — Информационная безопасность автоматизированных систем
Направленность: обеспечение информационной безопасности распределенных информационных систем
Формы обучения: очная

Курган 2018

Рабочая программа дисциплины «Безопасность сетей ЭВМ» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения « 31 » августа 2018 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 26 сентября 2018 года, протокол № 3.

Рабочую программу составил:
канд.тех.наук, доцент Д.И. Дик

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент Е.Н. Полякова

Начальник Управления
образовательных программ С.Н. Синицын

Специалист по учебно-методической
работе Управления образовательных
программ Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 7 зачетных единиц трудоемкости (252 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр	
		5	6
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**142**	**68**	**74**
Лекции	64	34	30
Лабораторные работы	64	34	30
Практические занятия	14	-	14
Самостоятельная работа, всего часов в том числе:	**110**	**40**	**70**
Подготовка к зачету	18	18	-
Подготовка к экзамену	45	-	45
Курсовая работа	15	-	15
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	32	22	10
Вид промежуточной аттестации	**зачет, экзамен**	**зачет**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**252**	**108**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Безопасность сетей ЭВМ» относится к базовым дисциплинам Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Основы теории защиты информации
- Основы информационной безопасности
- Организация ЭВМ и вычислительных систем.

Результаты обучения служат основой для дисциплин «Сети и системы передачи информации», «Разработка и эксплуатация защищенных автоматизированных систем», «Методы проектирования защищенных распределенных информационных систем», «Техническая защита информации», «Управление информационной безопасностью» и применяются для выполнения курсов работ и проектов и выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины является обучение студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

Задачи дисциплины:

- получение представления о программно-аппаратных и технических средств создания сетей;
- принципы построения сетей и управления ими;
- правила технической защиты сетей;
- использование программных и аппаратных технологий защиты сетей;
- методы проектирования, развертывания и сопровождения безопасных сетей;
- методы обследования и анализа защищенных вычислительных сетей.

Компетенции, формируемые в результате освоения дисциплины:

- способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способность проводить анализ защищенности автоматизированных систем (ПК-3);
- способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

В результате изучения дисциплины обучающийся должен:

знать:

- основные протоколы компьютерных сетей (для ПК-3, ПК-26);
- последовательность и содержание этапов построения компьютерных сетей (для ПК-9);

уметь:

- конфигурировать активное сетевое оборудование (ОПК-8).

- проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети (для ПК-26);

- эффективно использовать различные методы и средства защиты информации для компьютерных сетей (для ПК-3, ПК-4);

- проводить мониторинг угроз безопасности компьютерных сетей (для ПК-3, ПК-4, ПК-9);

владеть:

- навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности (для ПК-3, ПК-4, ПК-9);

- навыками эксплуатации и администрирования баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности (для ПК-9, ПК-26).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем		
			Лекции	Лабораторные работы	Практические занятия
5 семестр					
Рубеж 1		Введение. Функции сетей. Модель OSI	2	-	-
	1	Локальные сети. Принципы построения локальных сетей	2	-	-
	2	Сети Ethernet	2	4	-
	3	Стек протоколов TCP/IP. Логическая адресация в сетях TCP/IP.	4	4	-
	4	Служебные протоколы в сетях TCP/IP	4	-	-
	5	Трансляция сетевых адресов(NAT)	6	6	-
Рубеж 2	6	Сети IPv6	2	-	-
	7	Маршрутизация в сетях TCP/IP	8	20	-
	8	Служба доменных имен	2	-	-
	9	NetBIOS и WINS	2	-	
		Итого:	**34**	**34**	-
6 семестр					
Рубеж 1	10	Типовые угрозы сетевой безопасности	2	-	-
	11	Атаки на распределенные вычислительные системы	4	6	-
	12	Атаки на узлы вычислительных сетей	4	10	-
	13	Защита от несанкционированного проникновения	4	4	-
Рубеж 2	14	Защита сетей на уровне IP	4	4	2
	15	Защита World Wide Web	4	2	2
	16	Аутентификации в сетях	4	2	4
	17	Защита на прикладном уровне	4	2	6
		Итого:	**30**	**30**	**14**
		Всего за 5 и 6 семестр	**64**	**64**	**14**

4.2. Содержание лекционных занятий

Введение. Функции сетей. Модель OSI

Цели, предмет и задачи курса. Общие сведения о вычислительных сетях. Классификация вычислительных сетей. Базовая эталонная модель взаимодействия открытых сетей (модель OSI). Функции уровней модели OSI.

Преобразование данных при передаче по сети. Способы контроля правильности передачи информации.

Топологии вычислительных сетей.

Тема 1. Локальные сети. Принципы построения локальных сетей.

Локальные вычислительные сети. Методы управления доступом к среде передачи (коллективный доступ к среде передачи с прослушиванием несущей и обнаружением конфликтов, управляющий маркер, размеченное кольцо).

Тема 2. Сети Ethernet

Принципы построения сетей Ethernet. Методы доступа к среде передачи в сетях Ethernet. Адресация в сетях Ethernet. Формат Ethernet фрейма. Концентраторы, коммутаторы и принципы их работы.

Топологии соединения коммутаторов. Агрегирование портов коммутаторов. Алгоритм работы STP.

Виртуальные локальные сети (VLAN) и принципы их построения.

Тема 3. Стек протоколов TCP/IP. Логическая адресация в сетях TCP/IP.

Обзор стека протоколов TCP/IP. Адресация в сетях TCP/IP. Формат адреса IPv4. Классы IP адресов. Зарезервированные классы сетей. Адресация подсетей. Зарезервированные адреса в подсети. Маскирование подсетей. Планирование подсетей.

Формат IPv4 дейтаграммы.

Протокол UDP

Тема 4. Служебные протоколы в сетях TCP/IP

Протокол ARP: ARP-запросы, ARP-ответы, ARP-таблицы. Протокол RARP. Маршрутизаторы и ARP-таблицы. Шлюз по умолчанию.

Протокол ICMP. Групповое вещание. Протокол IGMP.

Протокол DHCP.

Тема 5. Трансляция сетевых адресов (NAT)

Назначение и виды трансляции сетевых адресов. Статическая трансляция сетевых адресов. Динамическая трансляция сетевых адресов. Трансляция сетевых адресов на уровне портов. Типы трансляции адресов на уровне портов: symmetric NAT, full cone NAT, address restricted cone NAT, port restricted cone NAT, hairpin NAT. Статическая трансляция сетевых адресов на уровне портов. Балансировка нагрузки с помощью NAT.

Определение способа трансляции адресов. Протокол STUN.

Проблемы, связанные с трансляцией адресов.

Тема 6. Сети IPv6

Отличие сетей IPv6 от сетей IPv4. Адресация в сетях IPv6. Префиксы адресов IPv6.

Формат заголовка IPv6. Дополнительные заголовки IPv6.

Автоконфигурирование адресов. Протокол ICMPv6. Исследование соседей в IPv6.

Тема 7. Маршрутизация в сетях TCP/IP

Маршрутизация с использованием сетевых адресов. Протоколы маршрутизации и маршрутизируемые протоколы. Операции, выполняемые протоколом сетевого уровня. Многопротокольная маршрутизация. Статические и динамические маршруты. Адаптация к изменениям топологи. Операции динамической маршрутизации. Представление расстояния с помощью метрики.

Алгоритмы маршрутизации. Централизованные и децентрализованные. Внутренние и внешние протоколы маршрутизации.

Протоколы маршрутизации. Алгоритмы маршрутизации по вектору расстояния. Алгоритм маршрутизации по вектору расстояния и исследование сети. Алгоритм маршрутизации по вектору расстояния и изменения топологии. Маршрутизация по замкнутому кругу. Счет до бесконечности.

Протокол маршрутизации RIP.

Алгоритмы маршрутизации с учетом состояния канала связи. Режим исследования сети в алгоритмах с учетом состояния канала. Обработка изменений топологии в протоколах маршрутизации с учетом состояния канала связи.

Протокол маршрутизации OSPF.

Автономные системы. Протоколы маршрутизации EBGP и IBGP.

Тема 8. Служба доменных имен

Иерархия узлов и доменов. Делегирование. Домены и зоны. Прохождение запроса клиента.

Типы серверов имен: основные, дополнительные, только для кэширования, узлы пересылки и подчиненные сервера.

Синтаксис записей ресурсов.

Динамическая DNS.

Тема 9. NetBIOS и WINS

Сетевая базовая система ввода-вывода NetBIOS. История и характеристики. Имена NetBIOS. Разрешение имен NetBIOS. Типы узлов NetBIOS. Служба обнаружения NetBIOS.

Служба имен Internet для Windows (WINS).

6 семестр. Технологии обеспечения безопасности в сетях

Тема 10. Типовые угрозы сетевой безопасности

Проблемы безопасности современных сетей. Классификация удаленных атак на распределенные вычислительные системы (по характеру воздействия, по цели воздействия, по условию начала осуществления воздействия, по наличию обратной связи с атакуемым объектом, по расположению субъекта атаки относительно атакуемого объекта, по уровню эталонной модели).

Характеристика и механизмы реализации типовых удаленных атак.

Тема 11. Атаки на распределенные вычислительные системы

Удаленные атаки на распределенные вычислительные системы: анализ сетевого трафика, ложный ARP сервер, ложный DNS сервер, навязывание лож-

ного маршрута с использованием протокола ICMP, подмена одного из субъектов TCP-соединения (hijacking), атаки типа отказ в обслуживании.

Тема 12. Атаки на узлы вычислительных сетей

Удаленные атаки на узлы вычислительных сетей. Переполнение буфера. Переполнение стека. Переполнение кучи. Ошибки индексации массивов. Ошибки в строках форматирования. Несовпадение размеров буфера.

SQL инъекции. Инъекции кода. Смешанные инъекции. Межсайтовый скриптинг. CSRF атаки.

Вредоносное программное обеспечение. Классификация вредоносного программного обеспечения. Вирусы, черви и трояны.

Тема 13. Защита от несанкционированного проникновения

Брандмауэры: характеристика, типы, конфигурации. Управление доступом к данным: понятие политики безопасности, типовые элементы политики безопасности, рекомендации по построению политики безопасности. Системы обнаружения и предотвращения вторжений. Защита от вредоносного программного обеспечения.

Тема 14. Защита сетей на уровне IP

Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Виртуальные частные сети. Концепция построения защищенных виртуальных частных сетей VPN. Функции и компоненты сети VPN. Туннелирование. Классификация виртуальных частных сетей VPN. Архитектура защиты на уровне IP. Протокол IPSec. Защищенные связи и их параметры. Протоколы AH и ESP. Транспортный и туннельный режимы.

Тема 15. Защита World Wide Web

Угрозы нарушения защиты Web. Протоколы SSL и TLS.

Тема 16. Аутентификации в сетях

Системы Kerberos версий 4 и 5: цели, диалог аутентификации, области и их взаимодействие. Служба аутентификации X.509: сертификаты и процедуры аутентификации.

Тема 17. Защита на прикладном уровне

Протокол SET. Протокол сетевого управления SNMP версий 1 и 2. Протокол сетевого управления SNMP версии 3. Система защиты электронной почты PGP. Система защиты электронной почты S/MIME. Архитектура систем аутентификации, авторизации и учета (AAA – Authentication, Authorization, Accounting). Протокол RADIUS.

4.3. Лабораторные работы

Номер темы	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
5 семестр			
2	Сети Ethernet	Настройка коммутатора	4
3	Стек протоколов TCP/IP. Логическая адресация в сетях TCP/IP	Фильтрация дейтаграмм	4

5	Трансляция сетевых адресов (NAT)	Трансляция сетевых адресов	4
	1-ый рубежный контроль	***Тестирование***	*2*
7	Маршрутизация в сетях TCP/IP	Основы настройки маршрутизаторов Cisco	4
		Статическая маршрутизация	6
		Настройка протокола маршрутизации RIP	4
	2-ой рубежный контроль	***Тестирование***	*2*
	Маршрутизация в сетях TCP/IP	Настройка протокола маршрутизации OSPF	4
	Итого		**34**
	6 семестр		
11	Атаки на распределенные вычислительные системы	Настройка сервера DNS	3
		Настройка сервера DHCP	3
12	Атаки на узлы вычислительных сетей	Настройка Active Directory	3
		SQL инъекции	3
		Межсайтовый скриптинг и CSRF атаки	4
13	Защита от несанкционированного проникновения	Исследование вредоносного программного обеспечения	4
14-17	Защита сетей на уровне IP. Защита World Wide Web. Аутентификации в сетях. Защита на прикладном уровне.	Настройка системы предотвращения вторжений	10
	Итого		**30**
	Всего за 5 и 6 семестры		***64***

4.4 Практические занятия

Номер темы	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
	6 семестр		
14,15	Защита сетей на уровне IP. Защита World Wide Web.	Методы и средства защиты информации (данных) в ИВС	2
	1-ый рубежный контроль	***Тестирование***	*2*
16,17	Аутентификации в сетях. Защита на прикладном уровне.	Защита информации в электронных платежных системах	4
		Управление доступом в ИВС. Электронная подпись.	4
	2-ой рубежный контроль	***Тестирование***	*2*
	Итого		**14**

Вопросы к семинарам

Методы и средства защиты информации (данных) в ИВС

1. Формальные средства защиты.
2. Физические средства защиты.
3. Аппаратные средства защиты.
4. Программные средства защиты.
5. Неформальные средства защиты.

6. Организационные средства защиты.
7. Законодательные меры защиты.
8. Морально-этические нормы.
9. Аппаратно-программные средства защиты информации в ПЭВМ.
10. Вирусы и антивирусы.
11. Обеспечение целостности информации, передаваемой в сетях ЭВМ.

Защита информации в электронных платежных системах

1. Платежные системы и пластиковые карты.
2. Персональный идентификационный номер (ПИН).
3. Безопасность систем POS.
4. Безопасность банкоматов.
5. Защищенная платежная система UEPS.
6. Безопасность платежей через сеть Ethernet.

Управление доступом в ИВС. Электронная подпись.

1. Идентификация и установление подлинности.
2. Проверка полномочий субъектов на доступ к ресурсам.
3. Регистрация обращений к защищенным ресурсам.
4. Реагирование на несанкционированные действия.
5. Однонаправленные хэш-функции.
6. Алгоритмы электронной цифровой подписи.

4.5 КУРСОВАЯ РАБОТА

Тема курсовой работы: «Проектирование локальной вычислительной сети организации».

Целью курсовой работы является реализация полученных знаний по дисциплине "Безопасность сетей ЭВМ".

Задание:

1. Спроектировать локальную вычислительную сеть организации в соответствии с индивидуальным заданием.
2. Подобрать для сети активное сетевое оборудование.
3. Составить смету.
4. Построить модель угроз для спроектированной сети.

Курсовая работа выполняется в соответствии с индивидуальным заданием. Объем курсовой работы 20-25 страниц.

Структура курсовой работы:

1) Титульный лист.
2) Оглавление (содержание) курсового проекта.
3) Введение.
4) Постановка задачи:
   а) исходные данные;
   б) цель курсовой работы;
   в) задачи, подлежащие рассмотрению (решению) в курсовой работе.
5) Содержательная часть (может быть в виде глав, разделов, параграфов, привязанных к задачам курсовой работы).

6) Заключение и выводы:

а) перечень полученных результатов (согласно цели и задачам курсовой работы) и их новизна;

б) выводы, полученные по итогам курсовой работы.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работы.

Залогом качественного выполнения лабораторных и практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано на лабораторных и практических занятиях коллективное взаимодействие и разбор конкретных ситуаций, а также обсуждение неясных моментов и ситуаций по лекционному курсу.

Для текущего контроля успеваемости преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных и практических занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, выполнение курсовой работы, подготовку к практическим и лабораторным занятиям, к рубежным контролям, подготовку к зачету и экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Подготовка к лабораторным работам	18
Подготовка к практическим занятиям	6
Подготовка к рубежным контролям (по 2часа)	8
Подготовка к зачету	18
Курсовая работа	15
Подготовка к экзамену	45
Всего:	110

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной формы обучения)

2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Банк тестовых заданий к рубежным контролям № 1, № 2, №3 и №4.
5. Курсовая работа.
6. Перечень вопросов к зачету и экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="8">Содержание</td></tr>
<tr><td rowspan="11">1</td><td rowspan="11">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="8">Распределение баллов</td></tr>
<tr><td colspan="8">5 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td colspan="2">Выполнение и защита лабораторной работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td colspan="2">зачет</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ x 17= $17_б$</td><td colspan="2">$5_б$ x 7 = $35_б$</td><td>9</td><td>9</td><td colspan="2">30</td></tr>
<tr><td colspan="8">6 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита лабораторной работы</td><td>Выполнение практической работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td colspan="2">экзамен</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ x 15 =$15_б$</td><td>$5_б$ x 7 = $35_б$</td><td>$2_б$ x 3 = $6_б$</td><td>7</td><td>7</td><td colspan="2">30</td></tr>
<tr><td colspan="8">Курсовая работа</td></tr>
<tr><td>Качество пояснительной записки</td><td>Качество проектной части</td><td colspan="2">Ритмичность выполнения</td><td colspan="2">Качество защиты</td><td colspan="2">Всего</td></tr>
<tr><td>до 20</td><td>до 30</td><td colspan="2">до 20</td><td colspan="2">до 30</td><td colspan="2">100</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета</td><td colspan="8">60 и менее баллов – неудовлетворительно; незачет;
61…73 – удовлетворительно; зачет;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="8">Для допуска к промежуточной аттестации (зачету, экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и практические работы, а также курсовую работу в 6 семестре.
Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов:
- 61 балл для получения «автоматически» зачета;
- 68 баллов для получения «автоматически» оценки удовлетворительно».
По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных и практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных и практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету или экзамену) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных и практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенных лабораторных и практических работ – до 9 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования. Зачет и экзамен проводится в традиционной форме.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

На каждое тестирование при рубежном контроле студенту отводится 2 часа. Варианты тестовых заданий для рубежных контролей №1, №2 состоят из 18 вопросов, а для рубежных контролей №3 и №4 — из 14 вопросов.

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости. Зачет проводится в форме ответов на 2 вопроса преподавателя. Экзаменационный билет состоит из 2-х вопросов, каждый их которых оценивается в 15 баллов. Время, отводимое студенту на подготовку к ответу на вопросы составляет 1 астрономический час.

Результаты текущего контроля успеваемости, зачета, курсовой работы и экзамена заносятся преподавателем в зачетную или экзаменационную ведомости, которая сдается в деканат факультета в день зачета, защиты курсовой работы и экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, зачета и экзамена

5 СЕМЕСТР

1-ый рубежный контроль

1. Что использует канальный уровень для поиска хоста в локальной сети?

1. Логическую сетевую адресацию
2. Номера портов
3. Аппаратные адреса
4. Шлюз по умолчанию

2. В каком режиме коммутатор локальной сети перед перенаправлением кадра проверяет только аппаратный адрес?

1. Сквозном
2. Сохранить и передать
3. Проверки фрагментов
4. Без фрагментов

3. Какой протокол обеспечивает службу с установлением соединения для взаимодействия хостов?

1. IP
2. ARP
3. TCP
4. UDP

2-ой рубежный контроль

1. На каком уровне OSI биты преобразуются в цифровые сигналы?

1. Физическом
2. Транспортном
3. Канальном
4. Сетевом

2. Что определяет в сети корневой коммутатор при использовании STP?

1. Приоритет
2. Стоимость подключенных к переключателю связей
3. MAC-адрес
4. IP-адрес

3. Если хост посылает в широковещательной рассылке кадр, содержащий аппаратный адрес источника и назначения, причем целью является присваивание себе IP-адреса, то какой используется протокол сетевого уровня?

1. RARP
2. ARP
3. ICMP
4. TCP
5. IPX

6 СЕМЕСТР

1-ый рубежный контроль

1. Какая метрика маршрутизации используется в протоколе RIP?

1. Счет до бесконечности
2. Счетчик участков
3. Время жизни TTL
4. Полоса пропускания, задержка

2. Какой алгоритм маршрутизации используется в протоколе RIP?

1. Маршрутизируемой информации
2. Связывания
3. Состояния связи
4. Дистанционно-векторный

3. Атака внедрения ложного ARP сервера является?

1. Пассивной.
2. Активной.
3. Межсегментной.
4. Внутрисегментной.

2-ой рубежный контроль

1. Какое из утверждений верно для межсетевого экран прикладного уровня?

2. Обычно требует модификации клиента для работы через межсетевой экран
3. Для обеспечения работы любой новой службы требуется только изменение конфигурации межсетевого экрана

2. Протокол SSL предназначен для

1. Защиты передачи данных с использованием протокола IP
2. Защиты передачи данных с использованием протокола TCP
3. Защиты передачи данных с использованием протокола UDP
4. Защиты сообщений электронной почты

3. Какое из описаний конфликта в сети Ethernet является наилучшим?

1. Результат передачи данных в сеть двумя узлами независимо друг от друга.
2. Результат одновременной передачи данных в сеть двумя узлами.
3. Результат повторной передачи данных в сеть двумя узлами
4. Результат невыполнения передачи данных в сеть двумя узлами.

Примерный перечень вопросов к зачету

1 Сеть Ethernet. Принципы работы. Концентраторы и коммутаторы.
2 Топологии соединения коммутаторов: остовное дерево (Spanning Tree), дублирующие линии (Resilient Link, LinkSafe), объединение портов (Port Trunking)
3 Виртуальные локальные сети (VLAN)
4 IP-адресация IPv4 (классовая и бесклассовая адресация, подсети, маска сети)
5 IP-адресация IPv6
6 Автоконфигурирование IP-адресов и обнаружение соседей в IPv6
7 Групповое вещание (протокол IGMP)
8 Служба доменных имен DNS
9 Протокол DHCP
10 Протокол ICMP
11 Протоколы ARP и RARP
12 Протокол UDP
13 Протокол TCP. Рукопожатие. Подтверждение передачи и повторная передача. Управление потоком и контроль перегрузки
14 Трансляция адресов (NAT)
15 Назначение и принципы работы протокола STUN

16 Алгоритмы маршрутизации. Централизованные и децентрализованные. Внутренние и внешние протоколы маршрутизации
17 Алгоритм маршрутизации RIP.
18 Алгоритм маршрутизации OSPF.
19 Алгоритм маршрутизации BGP.

Примерный перечень вопросов к экзамену

1 Сеть Ethernet. Принципы работы. Концентраторы и коммутаторы.
2 Топологии соединения коммутаторов: остовное дерево (Spanning Tree).
3 Топологии соединения коммутаторов: дублирующие линии (Resilient Link, LinkSafe).
4 Топологии соединения коммутаторов: объединение портов (Port Trunking).
5 Виртуальные локальные сети (VLAN).
6 IP-адресация IPv4 (классовая и бесклассовая адресация).
7 IP-адресация IPv4 (подсети, маска сети).
8 IP-адресация IPv6
9 Автоконфигурирование IP-адресов и обнаружение соседей в IPv6
10 Групповое вещание (протокол IGMP)
11 Служба доменных имен DNS
12 Протокол DHCP
13 Протокол ICMP
14 Протоколы ARP и RARP
15 Протокол UDP
16 Протокол TCP. Рукопожатие.
17 Подтверждение передачи и повторная передача.
18 Управление потоком и контроль перегрузки.
19 Трансляция адресов (NAT)
20 Назначение и принципы работы протокола STUN
21 Алгоритмы маршрутизации.
22 Централизованные и децентрализованные.
23 Внутренние и внешние протоколы маршрутизации
24 Алгоритм маршрутизации RIP.
25 Алгоритм маршрутизации OSPF.
26 Алгоритм маршрутизации BGP.
27 Классификация удаленных атак на распределенные вычислительные системы (по характеру воздействия, по цели воздействия)
28 Классификация удаленных атак на распределенные вычислительные системы (по условию начала осуществления воздействия).
29 Классификация удаленных атак на распределенные вычислительные системы (по наличию обратной связи с атакуемым объектом).
30 Классификация удаленных атак на распределенные вычислительные системы (по расположению субъекта атаки относительно атакуемого объекта)
31 Классификация удаленных атак на распределенные вычислительные системы (по уровню эталонной модели).

32 Удаленные атаки на распределенные вычислительные системы: анализ сетевого трафика.
33 Удаленные атаки на распределенные вычислительные системы: (ложный ARP сервер).
34 Удаленные атаки на распределенные вычислительные системы: (ложный DNS сервер)
35 Удаленные атаки на распределенные вычислительные системы: (навязывание ложного маршрута с использованием протокола ICMP).
36 Удаленные атаки на распределенные вычислительные системы: (подмена одного из субъектов TCP-соединения (hijacking)).
37 Удаленные атаки на распределенные вычислительные системы: (атаки типа отказ в обслуживании.
38 Методы атаки узлов вычислительной системы.
39 Межсетевые экраны (брандмауэры) и их виды.
40 Системы обнаружения и предотвращения вторжений (IDS и IPS).
41 Защита информации на IP уровне. Протокол IPSec
42 Защита WEB информации. Протокол SSL (TLS).
43 Сертификаты X.509
44 Протокол SET
45 Протокол сетевого управления SNMP версий 1 и 2
46 Протокол сетевого управления SNMP версии 3
47 Система защиты электронной почты PGP
48 Система защиты электронной почты S/MIME
49 Архитектура систем аутентификации, авторизации и учета (AAA – Authentication).
50 Удаленные атаки на распределенные вычислительные системы: (Authorization)
51 Удаленные атаки на распределенные вычислительные системы: (Accounting).
52 Протокол RADIUS.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1 Олифер, В. Г. Компьютерные сети: принципы, технологии, протоколы [Текст] : учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. – 2-е изд. – СПб: Питер, 2003. – 864 с.

2 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: курс лекций [Текст] : учебное пособие :

для студентов вузов, обучающихся по специальности 510200 "Прикладная математика и информатика"/ О.Р. Лапонина; Интернет-университет информационных технологий. – М.: Интернет-Университет информационных технологий, 2005. – 605 с.

3 Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018. – 416 с. – Доступ из ЭБС «znanium.com».

7.2. Дополнительная учебная литература

1 Лапонина, О. Р. Межсетевое экранирование [Электронный ресурс] : учебное пособие / О.Р. Лапонина; Интернет-университет информационных технологий. – Электрон. дан. – М.: Интернет-Университет информационных технологий, 2006. – Режим доступа: свободный: https://www.intuit.ru/studies/courses/20/20/info, свободный. – Загл. с экрана.

2 Ермаков, А.Е. Основы конфигурирования корпоративных сетей Cisco [Электронный ресурс] : учеб. пособие / А.Е. Ермаков. – М. : УМЦ ЖДТ, 2013. – 247 с. – Доступ из ЭБС «Консультант студента».

3 Назаров, С. В. Администрирование локальных сетей Windows NT/2000/.NET [Электронный ресурс] : Учеб. пособие / С. В. Назаров. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2003. – 480 с. – Доступ из ЭБС «znanium.com».

4 Лапонина, О. Р. Протоколы безопасного сетевого взаимодействия [Электронный ресурс] : учебное пособие / О.Р. Лапонина; Интернет-университет информационных технологий. – Электрон. дан. – М.: Интернет-Университет информационных технологий, 2005. – Режим доступа: свободный: https://www.intuit.ru/studies/courses/59/59/info, свободный. – Загл. с экрана.

5 Мэйволд, Э. Безопасность сетей [Электронный ресурс] : учебное пособие / Э. Мэйволд; Интернет-университет информационных технологий. – Электрон. дан. – М.: Интернет-Университет информационных технологий, 2005. – Режим доступа: https://www.intuit.ru/studies/courses/102/102/info, свободный. – Загл. с экрана

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Дик Д.И. SQL-инъекция. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 9 с.

2. Дик Д.И. Исследование вредоносного программного обеспечения. Методические указания к выполнению лабораторной работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 25 с.

3. Дик Д.И. Настройка протокола маршрутизации OSPF. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 28 с.

4. Дик Д.И. Настройка протокола маршрутизации RIP. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 28 с.

5. Дик Д.И. Межсайтовый скриптинг и CSRF атаки. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2017. – 21 с.

6. Дик Д.И. Настройка Active Directory. Методические указания к выполнению лабораторной работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2017. – 33 с.

7. Дик Д.И. Основы настройки маршрутизаторов Cisco. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 25 с.

8. Дик Д.И. Настройка коммутатора. Методические указания к выполнению лабораторной работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 19 с.

9. Дик Д.И. Настройка сервера DHCP. Методические указания к выполнению лабораторной работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 14 с.

10. Дик Д.И. Настройка сервера DNS. Методические указания к выполнению лабораторной работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 22 с.

11. Дик Д.И. Настройка системы предотвращения вторжений. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2016. – 42 с.

12. Дик Д.И. Основы маршрутизации. Статическая маршрутизация. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2017. – 19 с.

13. Дик Д.И. Фильтрация дейтаграмм в маршрутизаторах CISCO. Лабораторный практикум по дисциплине «Безопасность сетей ЭВМ» для студентов очной формы обучения направления 10.05.03 «Информационная безопасность автоматизированных систем» / Д.И. Дик. – Курган : РИЦ КГУ, 2016. – 12 с.

14. Дик Д.И. Трансляция сетевых адресов. Методические указания к выполнению лабораторной работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2017. – 19 с.

15. Дик Д.И. Методические указания для практических занятий по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2017. – 6 с.

16. Дик Д.И. Проектирование вычислительной сети предприятия. Методические указания к выполнению курсовой работы по дисциплине «Безопасность сетей ЭВМ» для студентов программы специалитета 10.05.03 «Информационная безопасность автоматизированных систем» и программы бакалавриата 10.03.01 «Информационная безопасность» / Д.И. Дик. – Электрон. дан. – Курган : КГУ, 2017. – 11 с.

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Сайт дистанционного обучения в НОУ (Национальный Открытый Университет) «ИНТУИТ» содержит бесплатные курсы, программы повышения квалификации и профессиональной переподготовки, интересные доклады и другую полезную информацию http://www.intuit.ru.
2. Федеральный портал «Российское образование» http://www.edu.ru/
3. Информационный сайт, содержащий справочные материалы по информатике, которые включают в себя курс лекций, схемы, презентации, рефераты и др. informatikaplus.narod.ru
4. Сайт о высоких технологиях, новости индустрии из мира компьютерного «железа», тестовые испытания и обзоры оборудования IXBT.com.
5. Портал «Информационно-коммуникационные технологии в образовании» http://www.ict.edu.ru.

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

1. Графический сетевой эмулятор GNS3
2. Эмулятор рабочей станции Virtual PC Simulator
3. Виртуальная машина VMware Player
3. Telnet терминал Putty или TeraTerm
4. Сетевой анализатор WireShark
5. Среда программирования Visual C++
4. Пакет Open Office

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект. Для проведения практических и лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого: локальная сеть компьютеров на базе ПК Pentium с установленным программным обеспечением MS Windows XP и с возможностью выхода в Интернет. Для эффективной работы в рамках дисциплины рекомендуется иметь возможность работать с исходными текстами программ, сохраненными на съемных накопителях информации.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Безопасность сетей ЭВМ»

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Направленность:
Обеспечение информационной безопасности распределенных информационных систем

Трудоемкость дисциплины: 7 з.е. (252 академических часа)
Семестр: 5 и 6 (очная форма обучения)
Форма промежуточной аттестации: зачет, экзамен

Содержание дисциплины

Стек протоколов TCP/IP. IP-адресация. Базовые протоколы TCP/IP. Методы и протоколы маршрутизации. Организация вычислительных сетей на базе операционных систем Windows. Типовые угрозы сетевой безопасности. Внутренние злоумышленники в корпоративных сетях. Технологии обеспечения безопасности в компьютерных сетях. Защита сетей на уровне IP. Защита World Wide Web. Аутентификации в сетях. Защита от несанкционированного проникновения.