МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Высшая школа информационных технологий и информационных систем

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____ _____20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Механизмы защиты удалённого доступа Б1.В.ДВ.9

Направление подготовки: 09.03.03 - Прикладная информатика
Профиль подготовки:
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Иванов К.В.

Рецензент(ы):

Таланов М.О.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Таланов М. О.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Высшей школы информационных технологий и информационных систем:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 689515516

Казань
2016

Содержание

Программу дисциплины разработал(а)(и) старший преподаватель, к.н. Иванов К.В. кафедра интеллектуальной робототехники Высшая школа информационных технологий и информационных систем , KVIvanov@kpfu.ru

1. Цели освоения дисциплины

Цель курса:

- Дать обзор механизмов удалённого доступа в контексте изменения парадигмы обработки информации в различных системах;
- Ознакомить слушателей с механизмами и методами защиты удалённого доступа;
- Дать практические навыки установки и настройки механизмов защиты удалённого доступа.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.9 Дисциплины (модули)" основной образовательной программы 09.03.03 Прикладная информатика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Слушатели должны обладать знаниями и навыками, получаемыми в ходе освоения курсов "Компьютерные сети", "Операционные системы", "информационная безопасность".

Знания, полученные при изучении этой дисциплины, потребуются далее при написании выпускных квалификационных работ, а также в ходе осуществления производственной деятельности.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-5 (профессиональные компетенции)	способностью выполнять технико-экономическое обоснование проектных решений
ОПК-4 (профессиональные компетенции)	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате освоения дисциплины студент:

1. должен знать:

- принципы функционирования механизмов защиты информации, применяемых в ходе организации защищённого удалённого доступа;
- механизмы и методы защиты информации, применяемые при построении информационных систем, защите персональных компьютеров, серверов и мобильных устройств, использование которых подразумевает применение различных технологий удалённого доступа;
- возможности по комплексному применению различных механизмов защиты удалённого доступа;

2. должен уметь:

- настраивать наиболее популярные браузеры с целью защищённой работы в недоверенных сетях;

- настраивать свободно распространяемые прокси-сервера;
- настраивать и корректно применять межсетевые экраны, входящие в состав дистрибутивов ОС семейства Windows и Linux;
- настраивать и использовать технологии VPN (на примере open VPN)
- применять технологии защищённого терминального доступа;

3. должен владеть:

-навыками использования технологий межсетевого экранирования;

-навыками использования технологий построения виртуальных частных сетей;

-навыками применения надстроек безопасности наиболее популярных браузеров;

-навыками использования прокси серверов стороннего размещения, а также прокси-серверов собственной настройки.

- Применять изученные механизмы средства для обеспечения защиты информации, обрабатываемой в информационных системах, предусматривающих использование удалённого доступа;
- Проектировать информационные системы с учётом необходимости реализации механизмов защиты информации удалённого доступа.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 6 зачетных(ые) единиц(ы) 216 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 8 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Эволюция систем удалённого доступа. Парадигма удалённой и распределённой обработки информации	8	1	4	0	0	устный опрос
2.	Тема 2. Атаки на системы удалённого доступа и этапы их осуществления	8	2	2	0	0	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
3.	Тема 3. Обзор компонент подсистем удалённого доступа, определяющих уровень защищённости, на примере подсистемы терминального доступа	8	2-3	6	10	0	отчет контрольная работа
4.	Тема 4. Обзор механизмов защиты удалённого доступа.	8	3-4	4	0	0	устный опрос
5.	Тема 5. Механизмы и технологии управлением удалённым доступом	8		4	2	0	устный опрос
6.	Тема 6. Механизмы и технологии межсетевого экранирования	8	4-5	6	10	0	отчет тестирование
7.	Тема 7. Механизмы и технологии построения виртуальных частных сетей.	8	6	4	6	0	отчет устный опрос
8.	Тема 8. Сценарии совместного применения механизмов защиты удалённого доступа.	8	7-8	6	8	0	отчет контрольная работа
.	Тема . Итоговая форма контроля	8		0	0	0	экзамен
	Итого			36	36	0	

4.2 Содержание дисциплины

Тема 1. Эволюция систем удалённого доступа. Парадигма удалённой и распределённой обработки информации

лекционное занятие (4 часа(ов)):

Основные термины и определения. Майнфреймы и терминалы. Локальные вычислительные сети. Клиент-серверная архитектура. Двухзвенная и трёхзвенная архитектура. Серверные и центры обработки данных. Облачная инфраструктура. Эволюция от автоматизированных к информационным системам.

Тема 2. Атаки на системы удалённого доступа и этапы их осуществления

лекционное занятие (2 часа(ов)):

Определение атаки. Фазы атаки. Признаки атаки. Сетевые атаки и способы защиты от них.

Тема 3. Обзор компонент подсистем удалённого доступа, определяющих уровень защищённости, на примере подсистемы терминального доступа

лекционное занятие (6 часа(ов)):

Компоненты сети, определяющие уровень защищённости: Узлы (автоматизированные рабочие места и сервера) и их сетевые адаптеры. Активное сетевое оборудование. Структурированная кабельная система. Схема и описание подсистемы отказоустойчивого терминального доступа. особенности реализации Active Directory.

практическое занятие (10 часа(ов)):

1. Развёртывание контроллеров домена и службы Active Directory. 2. Развёртывание и настройка терминальных серверов. 3. Настройка посредника подключения к ферме терминальных серверов. 4. Инициализация фермы и создание пользователей.

Тема 4. Обзор механизмов защиты удалённого доступа.

лекционное занятие (4 часа(ов)):

Обзор механизмов и технологий аутентификации; Обзор механизмов и технологий разграничения удалённого доступа; Обзор механизмов и технологий шифрования.

Тема 5. Механизмы и технологии управлением удалённым доступом

лекционное занятие (4 часа(ов)):

Аутентификация субъектов и объектов; Аутентификация устройств и пользователей; Сетевой контроль доступа.

практическое занятие (2 часа(ов)):

Обзор средств разграничения доступа на активном сетевом оборудовании

Тема 6. Механизмы и технологии межсетевого экранирования

лекционное занятие (6 часа(ов)):

Определение и классификации межсетевых экранов. Основные компоненты межсетевых экранов. Механизмы межсетевого экранирования, используемые на разных уровнях модели OSI. Технологии, реализуемые на базе межсетевых экранов. Тестирование межсетевых экранов.

практическое занятие (10 часа(ов)):

1. Установка и настройка прокси сервера. 2.Изучение возможностей МЭ, встроенного в ОС семейства Windows, предназначенную для АРМ. 3. Изучение возможностей МЭ, встроенного в ОС семейства Windows, предназначенную для серверов. 4.Изучение возможностей межсетевого экрана iptables

Тема 7. Механизмы и технологии построения виртуальных частных сетей.

лекционное занятие (4 часа(ов)):

Определение и классификации VPN. Основные компоненты VPN. Технологии VPN. Тестирование VPN и типовые сценарии использования.

практическое занятие (6 часа(ов)):

1. Установка сервера OpenVPN. 2. Установка клиента OpenVPN. 3. Развёртывание VPN "сеть-сеть". 4.Развёртывание VPN "узел-узел".

Тема 8. Сценарии совместного применения механизмов защиты удалённого доступа.

лекционное занятие (6 часа(ов)):

Сопряжение политик МЭ и VPN. Варианты совместного подключения МЭ и VPN. Реализации архитектуры "Бастион" Реализация архитектуры "Демилитаризованная зона"

практическое занятие (8 часа(ов)):

1. Обеспечение защищённой работы с терминальной фермой. 2. Дополнение схемы установкой прокси-сервера. 3. Подключение к терминальной ферме с использованием технологии VPN

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Эволюция систем удалённого доступа. Парадигма удалённой и распределённой обработки информации	8	1	подготовка к устному опросу	10	устный опрос
2.	Тема 2. Атаки на системы удалённого доступа и этапы их осуществления	8	2	подготовка к устному опросу	8	устный опрос
3.	Тема 3. Обзор компонент подсистем удалённого доступа, определяющих уровень защищённости, на примере подсистемы терминального доступа	8	2-3	подготовка к контрольной работе	10	контрольная работа
				подготовка к отчету	10	отчет
4.	Тема 4. Обзор механизмов защиты удалённого доступа.	8	3-4	подготовка к устному опросу	10	устный опрос
5.	Тема 5. Механизмы и технологии управлением удалённым доступом	8		подготовка к устному опросу	10	устный опрос
6.	Тема 6. Механизмы и технологии межсетевого экранирования	8	4-5	подготовка к отчету	15	отчет
				подготовка к тестированию	5	тестирование
7.	Тема 7. Механизмы и технологии построения виртуальных частных сетей.	8	6	подготовка к отчету	8	отчет
				подготовка к устному опросу	2	устный опрос
8.	Тема 8. Сценарии совместного применения механизмов защиты удалённого доступа.	8	7-8	подготовка к контрольной работе	5	контрольная работа
				подготовка к отчету	15	отчет
	Итого				108	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и практических занятий, а также самостоятельной работы студентов. Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в книгах.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Эволюция систем удалённого доступа. Парадигма удалённой и распределённой обработки информации

устный опрос , примерные вопросы:

Майнфреймы и терминалы. Локальные вычислительные сети. Клиент-серверная архитектура. Двухзвенная и трёхзвенная архитектура. Серверные и центры обработки данных. Облачная инфраструктура.

Тема 2. Атаки на системы удалённого доступа и этапы их осуществления

устный опрос , примерные вопросы:

Атака. Фазы атаки. Деятельность нарушителя на каждой фазе атаки.

Тема 3. Обзор компонент подсистем удалённого доступа, определяющих уровень защищённости, на примере подсистемы терминального доступа

контрольная работа , примерные вопросы:

1.Свойства и уязвимости узлов сети. 2.Свойства и уязвимости коммутаторов 3. Свойства и уязвимости маршрутизаторов. 4. Доменные группы 5. Определение основных элементов инфраструктуры AD 6. Схема отказоустойчивой терминальной фермы серверов.

отчет , примерные вопросы:

1. Развёртывание контроллеров домена и службы Active Directory. 2. Развёртывание и настройка терминальных серверов. 3. Настройка посредника подключения к ферме терминальных серверов. 4. Инициализация фермы и создание пользователей.

Тема 4. Обзор механизмов защиты удалённого доступа.

устный опрос , примерные вопросы:

Механизмы и технологии аутентификации; Механизмы и технологии разграничения удалённого доступа; Механизмы и технологии шифрования.

Тема 5. Механизмы и технологии управлением удалённым доступом

устный опрос , примерные вопросы:

Обзор средств разграничения доступа на активном сетевом оборудовании

Тема 6. Механизмы и технологии межсетевого экранирования

отчет , примерные вопросы:

1. Установка и настройка прокси сервера. 2.Изучение возможностей МЭ, встроенного в ОС семейства Windows, предназначенную для АРМ. 3. Изучение возможностей МЭ, встроенного в ОС семейства Windows, предназначенную для серверов. 4.Изучение возможностей межсетевого экрана iptables

тестирование , примерные вопросы:

Определение и классификации межсетевых экранов. Основные компоненты межсетевых экранов. Механизмы межсетевого экранирования, используемые на разных уровнях модели OSI. Технологии, реализуемые на базе межсетевых экранов. Тестирование межсетевых экранов.

Тема 7. Механизмы и технологии построения виртуальных частных сетей.

отчет , примерные вопросы:

1. Установка сервера OpenVPN. 2. Установка клиента OpenVPN. 3. Развёртывание VPN "сеть-сеть". 4.Развёртывание VPN "узел-узел".

устный опрос , примерные вопросы:

Определение и классификации VPN. Основные компоненты VPN. Технологии VPN. Тестирование VPN и типовые сценарии использования.

Тема 8. Сценарии совместного применения механизмов защиты удалённого доступа.

контрольная работа , примерные вопросы:

1. Широкие и узкие фильтры политик МЭ и VPN. 2. Варианты совместного подключения МЭ и VPN. Последовательное и параллельное подключение. 3. Реализации архитектуры "Бастион" 4. Реализация архитектуры "Демилитаризованная зона"

отчет , примерные вопросы:

1. Обеспечение защищённой работы с терминальной фермой. 2. Дополнение схемы установкой прокси-сервера. 3. Подключение к терминальной ферме с использованием технологии VPN

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

Вопросы к экзамену:

1. Атака. Фазы атаки. Деятельность нарушителя на каждой фазе атаки.
2.Свойства и уязвимости узлов сети.
3.Свойства и уязвимости коммутаторов
4. Свойства и уязвимости маршрутизаторов.
5. Доменные группы
6. Определение основных элементов инфраструктуры AD
7. Схема отказоустойчивой терминальной фермы серверов.
8. Механизмы и технологии аутентификации.
9.Механизмы и технологии разграничения удалённого доступа.
10 Механизмы и технологии шифрования.
11.Определение и классификации межсетевых экранов.
12. Основные компоненты межсетевых экранов.
13. Механизмы межсетевого экранирования, используемые на разных уровнях модели OSI.
14. Определение и классификации VPN.
15. Основные компоненты VPN.
16. Типовые сценарии использования VPN.
17. Реализации архитектуры "Бастион"
18. Реализация архитектуры "Демилитаризованная зона"

7.1. Основная литература:

1. Ищейнов В. Я. Мецатунян М. В. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: 60x90 1/16. - (Профессиональное образование) (Обложка) ISBN 978-5-00091-079-5 http://znanium.com/catalog.php?bookinfo=508381

2.Колисниченко, Д. Н. Беспроводная сеть дома и в офисе [Электронный ресурс] : самоучитель / Д.Н. Колисниченко. ? СПб.: БХВ-Петербург, 2009. ? 454 с.: ил. ? (Самоучитель) - ISBN 978-5-9775-0427-0 http://znanium.com/catalog.php?bookinfo=489446

3. Максим, М. Безопасность беспроводных сетей [Электронный ресурс] / Мерритт Максим, Дэвид Поллино; Пер. с англ. А. В. Семенова. - М. : Компания АйТи : ДМК Пресс, 2008. - 288 с.: ил. - (Информационные технологии для инженеров). - ISBN 5-98453-007-4 (АйТи), ISBN 5-94074-248-3 (ДМК Пресс). http://znanium.com/catalog.php?bookinfo=408862

7.2. Дополнительная литература:

1. Агапов, А. В. Обработка и обеспечение безопасности электронных данных [Электронный ресурс] : учеб. пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. - М.: МФПУ Синергия, 2012. - 592 с. - (Сдаем госэкзамен). - ISBN 978-5-4257-0074-2. http://znanium.com/catalog.php?bookinfo=451354

2. Оглтри, Т. Firewalls. Практическое применение межсетевых экранов [Электронный ресурс] / Т. Оглтри; Пер. с англ. - М.: ДМК Пресс, 2008. - 400 с.: ил. - (Серия "Защита и администрирование"). - ISBN 5-94074-037-5. http://znanium.com/catalog.php?bookinfo=407600

7.3. Интернет-ресурсы:

База знаний по UserGate Proxy & Firewall - http://support.entensys.com/index.php?/ru/Knowledgebase/List/Index/

Библиотека Online - http://citforum.ru/

езависимый информационно-аналитический центр, посвященный информационной безопасности. - http://www.anti-malware.ru

Лаборатория сетевой безопасности - http://ypn.ru/

Эмулятор работы межсетевых экранов - http://www.fwbuilder.org/

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Механизмы защиты удалённого доступа" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной проекционным оборудованием. Лабораторные занятия проводятся в специализированных компьютерных кабинетах информатики и вычислительных технологий с выходом в Интернет и установленной интерактивной доской.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 09.03.03 "Прикладная информатика" .

Автор(ы):
Иванов К.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Таланов М.О. _____
"__" _____ 201 __ г.