Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

Утверждаю
Председатель Ученого совета,
Ректор КарГТУ
Газалиев А.М.
_____
«____» _____ 2013г.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА – SYLLABUS

Дисциплина ZSIT 4309 «Защита сетевых информационных технологий»

Модуль SS 28 «Системы и сети»

Специальность 5В100200 –
«Системы информационной безопасности»

Факультет информационных технологий
Кафедра Информационные технологии и безопасность

2013

Предисловие

Программа обучения по дисциплине для студента – syllabus разработана: старшим преподавателем кафедры ИТБ Бартосик Ф.М

Обсуждена на заседании кафедры «Информационные технологии и безопасность»

Протокол № _____ от «____»_____2013 г.
Зав. кафедрой _____ М.М. Коккоз «____»_____2013 г.

Одобрена учебно-методическим советом факультета информационных технологий

Протокол № _____ от «____»_____2013 г.
Председатель _____ Л.М. Мустафина «____»_____2013 г.

Сведения о преподавателе и контактная информация

Бартосик Феликс Михайлович, старший преподаватель кафедры ИТБ.

Кафедра ИТБ находится в главном корпусе КарГТУ (Б.Мира 56), аудитория 429, контактный телефон 56-75-92, доб 1028.

Трудоемкость дисциплины

Семестр	Количество кредитов	ECTS	Вид занятий					Количество часов СРС	Общее количество часов	Форма контроля
			количество контактных часов			количество часов СРСП	всего часов			
			лекции	практические занятия	лабораторные занятия					
7	3	5	15	-	30	45	90	45	135	Э

Характеристика дисциплины

Дисциплина «Защита сетевых информационных технологий» входит в цикл профилирующих дисциплин в качестве компонента по выбору в составе модуля «системы и сети».

В рамках данной дисциплины рассматриваются теоретические знания в области анализа угроз, подбора методов и средств их предотвращения и организации систем защиты компьютерных технологий и систем. Уровень обучения данной дисциплине должен соответствовать такому, который позволит использовать полученные знания и навыки в практической деятельности, научных исследованиях, при написании выпускной квалификационной работы.

Цель дисциплины

Дисциплина «Защита сетевых информационных технологий» ставит целью формирование у студентов знаний и умений по защите компьютерных сетей с применением современных программно-аппаратных средств.

Задачи дисциплины

Задачи дисциплины следующие: дать студентам необходимые знания о фундаментальных понятиях видеомонтажа.

В результате изучения данной дисциплины студенты должны:

иметь представление:

- об основных понятиях, используемых при защите информации в компьютерных сетях;
- об основных угрозах и проблемах защиты сетевых информационных технологий;
- о методах защиты информации в сетях различного назначения;

знать:

- технологии обнаружения компьютерных атак и их возможности;
- основные уязвимости и типовые атаки на современные компьютерные системы;
- возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;
- методы защиты компьютерных сетей;
- классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;
- основные принципы администрирования защищенных компьютерных систем;
- особенности реализации методов защиты и сохранения информации современными программно-аппаратными средствами;

уметь:

- выполнять функции администратора безопасности защищенных компьютерных систем;
- выполнять настройку защитных механизмов сетевых программно-аппаратных средств;
- настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;
- применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных сетей;
- организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;
- применять механизмы защиты беспроводных сетей.

приобрести практические навыки:

- администрирования сетевых программно-аппаратных комплексов защиты информации;
- администрирования систем обнаружения компьютерных атак;
- аудита средств и систем информационной безопасности;
- администрирования систем организации виртуальных частных сетей.

Пререквизиты

Для изучения данной дисциплины необходимо усвоение следующих дисциплин:

«Введение в защиту и безопасность информации», «Организация вычислительных систем и сетей», «Методы и средства защиты компьютерной информации».

Постреквизиты

Знания, полученные при изучении дисциплины «Защита сетевых информационных технологий» используются при дипломном проектировании.

Тематический план дисциплины

Наименование раздела, (темы)	Трудоемкость по видам занятий, ч.				
	лекции	практические	лабораторные	СРСП	СРС
Раздел 1. Введение в криптографию					
1. Симметричное шифрование	1			3	6
2. Шифрование с открытым ключом	1			3	6
3. Электронная цифровая подпись	1			3	
Раздел 2. Компьютерные атаки и их обнаружение					
1. Файловые вирусы	1			3	
2. Макровирусы	1			3	3
3. Сетевые черви	1			3	6

4. Загрузочные вирусы	1			3	3
5. Троянские кони	1			3	3
6. Технологии маскировки вирусов	1			3	3
7. Тенденции современных компьютерных вирусов	1				3
Раздел 3. Средства защиты сети					
1. Межсетевые экраны	1			6	6
2. Виртуальные частные сети (VPN)	2			6	6
3. Системы обнаружения вторжений (IDS)	2			6	
Лабораторные работы					
1. Разработка программ тестирования защитных процедур			10		
2. Разработка программы определения надежности защиты			10		
3. Разработка экспертной системы для контроля атаки			10		
ИТОГО:	15		30	45	45

Перечень лабораторных занятий

1. Разработка программ тестирования защитных процедур
2. Разработка программы определения надежности защиты
3. Разработка экспертной системы для контроля атаки

Темы контрольных заданий для СРС

Тематика рефератов

1. алгоритм DES.
2. алгоритм RSA.
3. Принцип действия сетевых червей
4. Предназначение межсетевых экранов
5. Каким образом проникают в систему макровирусы?
6. Какому требованию должен удовлетворять пароль для противодействия атаке по персональному словарю?
7. Как называются вирусы, которые автоматически запускаются в момент старта операционной системы и, таким образом, постоянно функционируют в оперативной памяти? Способы проникновения в систему, и методы предотвращения от заражения.
8. Какие виды антивирусов существуют, принципы работы.
9. Классы VPN-соединений, их различия.
10. Фишинг. Требования к паролю для противодействия.

Критерии оценки знаний студентов

Экзаменационная оценка по дисциплине определяется как сумма максимальных показателей успеваемости по рубежным контролям (до 60%) и итоговой аттестации (экзамен) (до 40%) и составляет значение до 100%.

График выполнения и сдачи заданий по дисциплине

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи	Баллы
Сдача лабораторной работы № 1	Проверка практических навыков	[1],[2],[3]	5 недель	Текущий	5-я неделя	10
Сдача лабораторной работы № 2	Проверка практических навыков	[1],[2],[3]	5 недель	Текущий	10-я неделя	10
Сдача лабораторной работы № 3	Проверка практических навыков	[1],[2],[3]	5 недель	Текущий	15-я неделя	10
Отчет по СРС	Углубление знаний по теме «Симметричное шифрование»	[1] стр.153-181 [2] стр. 400-440 [3] стр. 170-250	2 недели	Текущий	2-я неделя	3
Отчет по СРС	Углубление знаний по теме «Шифрование с открытым ключом»	[1] стр.260-280 [2] стр. 440-508 [3] стр. 250-260	2 недели	Текущий	4-я неделя	3
Отчет по СРС	Углубление знаний по теме «Макровирусы»	[1] стр.475-492 [2] стр. 249-266 [3] стр. 75-89	1 неделя	Текущий	5-я неделя	3
Отчет по СРС	Углубление знаний по теме «Сетевые черви»	[1] стр.475-492 [2] стр. 249-266 [3] стр. 75-89	2 недели	Текущий	7-я неделя	3
Отчет по СРС	Углубление знаний по теме «Загрузочные вирусы»	[1] стр.475-492 [2] стр. 249-266 [3] стр. 75-89	1 неделя	Текущий	8-я неделя	3

Отчет по СРС	Углубление знаний по теме «Троянские кони»	[1] стр.239-259 [2] стр. 160-175 [3] стр. 150-170	1 неделя	Текущий	9-я неделя	3
Отчет по СРС	Углубление знаний по теме «Технологии маскировки вирусов»	[1] стр.475-492 [2] стр. 249-266 [3] стр. 75-89	1 неделя	Текущий	10-я неделя	3
Отчет по СРС	Углубление знаний по теме «Тенденции современных компьютерных вирусов»	[1] стр.103-120 [2] стр. 290-320 [3] стр. 106-155	1 неделя	Текущий	11-я неделя	3
Отчет по СРС	Углубление знаний по теме «Межсетевые экраны»	[1] стр.475-492 [2] стр. 249-266 [3] стр. 75-89	2 недели	Текущий	13-я неделя	3
Отчет по СРС	Углубление знаний по теме «Виртуальные частные сети (VPN)»	[1] стр.120-153 [2] стр. 209-235 [3] стр. 205-238	2 недели	Текущий	15-я неделя	3
Экзамен	Проверка усвоения материала дисциплины	Весь перечень основной и дополнительной литературы	2 контактных часов	Итоговый	В период сессии	40
Итого						100

Политика и процедуры

При изучении дисциплины «Защита сетевых информационных технологий» прошу соблюдать следующие правила:

1 Не опаздывать на занятия.

2 Не пропускать занятия без уважительной причины, в случае болезни прошу представить справку, в других случаях – объяснительную записку.

3 В обязанности студента входит посещение всех видов занятий.

4 Согласно календарному графику учебного процесса сдавать все виды контроля.

5 Пропущенные практические и лабораторные занятия отрабатывать в указанное преподавателем время.

6 Активно участвовать в учебном процессе.

7 Осуществлять поиск и обработку материалов Интернет и периодической печати о изучаемом предмете.

Список основной литературы

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие.–М.: Форум: Инфра-М, 2010.-592с.
2. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: -М. :ВШЭ,2011.-576
3. Краковский Ю.М Информационная безопасность и защита информации: Учебный курс.- М.: Форум: ИКЦ "МарТ", 2008.-288с.

Список дополнительной литературы

1. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита инфор-мации в персональном компьютере: - М.: Форум, 2009г.-368с.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М.: Академия, 2008г. – 256с
3. Колисниченко Д. Н. Rootkits под Windows. Теория и практика программирования "шапок-невидимок", позволяющих скрывать от системы данные, процессы, сетевые соединения. - СПб.: Наука и Техника. 2006. -320 с: ил.
4. Зайцев О. В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. — СПб.: БХВ-Петербург, 2006. — 304 с: ил.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

по дисциплине ZSIT 4309 «Защита сетевых информационных технологий»

Модуль SS 28 «Системы и сети»

Гос.изд.лиц. №50от.31.03.2004

Подписано к печати _____ 20___. г. Формат 60х90/16 Тираж _____ экз.

Объем _____ уч. изд. л. Заказ №_____ Цена договорная

100027 Издательство КарГТУ, Караганда, Бульвар Мира, 56