Министерство образования и науки Республики Казахстан

Карагандинский государственный технический университет

«Утверждаю»
Председатель Ученого совета,
ректор, академик НАН РК
Газалиев А.М.
_____
«____» _____2015 г

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ МАГИСТРАНТА (SYLLABUS)

Дисциплина **SB 4222** Сетевая безопасность

Модуль **SBI 25** Сетевая безопасность и Интернет

Специальность 5В070400 – Вычислительная техника
и программное обеспечение

Факультет Информационные технологии

Кафедра Информационно-вычислительных систем

2015

Предисловие

Программа обучения по дисциплине **SB 4222** Сетевая безопасность для студента (syllabus) разработана в соответствии с рабочим учебным планом, утвержденным решением Ученого совета (протокол №13 от 02.07.2012 г.) и типовой учебной программой по специальности 5В070400 – «Вычислительная техника и программное обеспечение» к.т.н., доцентом Когай Г.Д., доц. Ким В.В.

Обсуждена на заседании кафедры информационно-вычислительных систем

Протокол № 1 от « 28 » 08 2015 г.

Зав. кафедрой Амиров А.Ж. _____ « 28 » 08 2015 г.
(подпись)

Одобрена методическим советом факультета информационных технологий:

Протокол № 1 от « 1 » 09 2015 г.

Председатель Капжаппарова Д.У. _____ « 1 » 09 2015 г.
(подпись)

Сведения о преподавателе и контактная информация

Ф.И.О. Когай Галина Давыдовна, к.т.н., доктор PhD, доцент

Ученая степень, звание, должность

Ким В.В., к.т.н., доцент _____

Кафедра ИВС находится в гл. корпусе КарГТУ (Бульвар Мира 56), аудитория 301, контактный телефон 56-75-98 , доп. (2054).

Трудоемкость дисциплины

Семестр	Количество кредитов	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					
8	3	5	15	15	15	45	90	45	135	КП Экзамен

Характеристика дисциплины

Дисциплина «Сетевая безопасность» входит в цикл базовых дисциплин (компонент по выбору) рабочего учебного плана по специальности 5В070400 «Вычислительная техника и программное обеспечение».

Цель дисциплины

Целью дисциплины «Сетевая безопасность» является изучение основных принципов построения современных программных средств защиты информации.

Задачи дисциплины

- Задачи дисциплины следующие:
- ознакомление магистрантов с технологиями защиты информации в персональном компьютере;
- приобретение навыков организации криптографических методов защиты информации;
- приобретение навыков борьбы с угрозами несанкционированного доступа к информации;
- умение оценить правовое обеспечение информационной безопасности.

В результате изучения данной дисциплины студенты должны:

Знать:

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа.

Изучить:

- способы защиты информации в персональном компьютере;
- методы криптографического преобразования информации;
- методы антивирусной защиты информации;
- состав и методы правовой защиты информации.

Уметь:

– применять правовые, организационные, технические и программные средства защиты информации;
– создавать программные средства защиты информации.

Знания, полученные в процессе изучения дисциплины, ориентированы на решение задач проектирования систем и сетей; администрирования и планирования систем сетевой безопасности.

1.6 Пререквизиты

Для изучения данной дисциплины необходимо усвоение следующих дисциплин:
1. Математический анализ;
2. Операционные системы и среды;
3. Организация вычислительных систем и сетей;
4. Программирование на алгоритмических языках;
5. Компьютерные сети.

1.7 Постреквизиты

Знания, полученные при изучении дисциплины «Сетевая безопасность», используются при написании дипломного проекта.

Тематический план дисциплины

Наименование раздела (темы)	Трудоемкость по видам занятий, ч.				
	лекции	практи-ческие	лабора-торные	СРСП	СРС
1. Введение	1				
2. Актуальность проблемы обеспечения безопасности сети					
2.1 Угрозы информационной безопасности. Классификация угроз.	2			3	3
2.2 Распространение объектно-ориентированного подхода на информационную безопасность	2			4	4
3. Защита от воздействия вирусов. Антивирусные программы.	2			4	4
3.1 Проблема вирусного заражения и структура современных вирусов.	2			4	4
3.2 Способы заражения программ.	2			4	4
3.3 Классификация антивирусных программ.	2			4	4

4. Виды мер обеспечения информационной безопасности	2			4	4
4.1 Административный уровень защиты информации	2			4	4
5. Методы криптографических преобразований данных.	2			4	4
5.1 Шифры замены.	2			4	4
5.2 Шифры перестановки.	2			4	4
5.3 Шифрование методом гаммирования и с помощью аналитического преобразования.	2			4	4
5.4 Стандарты шифрования.	2			4	4
6. Особенности защиты информации в ПК	2			4	4
6.1 Защита ПК от несанкционированного доступа.	2			4	4
6.2 Программные средства защиты информации.	2			4	4
6.3 Протоколирование и аудит.	2			4	4
6.4 Управление доступом.	2			4	4
Практическое занятие №1. Консоль управления Windows Server 2003..		1		4	4
Практическое занятие №2: Управление учетными записями пользователей.		2		4	4
Практическое занятие №3: Управление учетными записями групп и компьютеров.		2			
Практическое занятие №4: Файлы и папки. Управление данными.		2			
Практическое занятие №5: Архивация данных.		2			
Практическое занятие №6: Обслуживание операционной системы.		2			
Практическое занятие №7: Управление оборудованием и драйверами.		2			
Лабораторная работа №1. Реализация методов защиты			1		

программного обеспечения от несанкционированного доступа					
Лабораторная работа №2. Реализация алгоритма шифрования методами перестановок			2		
Лабораторная работа №3. Реализация много петлевого алгоритма шифрования			2		
Лабораторная работа №4. Реализация датчика псевдослучайных чисел (ДПЧ)			2		
Лабораторная работа №5. Знакомство с существующими системами идентификации и аутентификации пользователей			2		
Лабораторная работа №6. Ознакомление с методами и средствами антивирусной защиты			2		
Лабораторная работа №7. Безопасность компьютерных сетей			2		
ИТОГО	**15**	**15**	**15**	**45**	**45**

Перечень самостоятельных работ

1. Угрозы информационной безопасности. Классификация угроз.
2. Распространение объектно-ориентированного подхода на информационную безопасность
3. Проблема вирусного заражения и структура современных вирусов.
4. Способы заражения программ
5. Классификация антивирусных программ.
6. Административный уровень защиты информации
7. Шифры замены.
8. Шифры перестановки.
9. Шифрование методом гаммирования и с помощью аналитического преобразования.
10. Стандарты шифрования.
11. Защита ПК от несанкционированного доступа.
12. Программные средства защиты информации.
13. Управление доступом.
14. Защита информации от копирования.
15. Акустические каналы утечки информации. Воздушные, вибрационные, электроакустические, оптико-электронные и параметрические каналы.

Перечень лабораторных занятий

Лабораторная работа №1. Реализация методов защиты программного обеспечения от несанкционированного доступа.

Лабораторная работа №2. Реализация алгоритма шифрования методами

перестановок

Лабораторная работа №3. Реализация много петлевого алгоритма шифрования

Лабораторная работа №4. Реализация датчика псевдослучайных чисел (ДПЧ)

Лабораторная работа №5. Знакомство с существующими системами идентификации и аутентификации пользователей.

Лабораторная работа №6. Ознакомление с методами и средствами антивирусной защиты.

Лабораторная работа №7. Безопасность компьютерных сетей.

Перечень практических занятий

Практическое занятие №1. Построение системы защиты информации. Ядро СЗИ. Ресурсы СЗИ. Организационное построение СЗИ.

Практическое занятие №2. Акустические каналы утечки информации. Воздушные, вибрационные, электроакустические, оптико-электронные и параметрические каналы.

Практическое занятие №3**.** Этапы проектирования СЗИ и их общее содержание. Понятие встроенной и добавочной защиты. Подходы к построению добавочной защиты.

Практическое занятие №4. Архитектура системы защиты. Явные и скрытые угрозы. Сетевые атаки. Функциональная модель системы защиты. Состав и назначение функциональных блоков.

Практическое занятие №5. Политика безопасности. Политика информационной безопасности предприятия. Шаги разработки политики информационной безопасности. Служба информационной безопасности. Разработка сетевых аспектов политики безопасности.

Практическое занятие №6. Политика безопасности ЛВС, ее цели, распределение ролей и обязанностей. Восстановление системы. Антивирусная защита.

Практическое занятие №7. Шлюзы сеансового уровня, прикладного уровня и SPI брандмауэры. Проверка пакетов с фиксацией состояния. Назначение, принцип работы, преимущества и недостатки.

Тематический план самостоятельной работы студента с преподавателем (СРСП)

Наименование темы СРМП	Цель занятия	Форма проведения занятия	Содержание задания	Рекомендуемая литература
Угрозы информационной безопасности. Классификация угроз.	Углубление знаний по данной теме	Выполнение упражнений	Модели, принципы, подходы управления доступом	[8,10]
Распространение объектно-ориентированного подхода на информационную безопасность	Углубление знаний по данной теме	Выполнение упражнений	Реализация моделей управления доступом с помощью принци-пов добавочной и втроенной защиты	[10]

Проблема вирусного заражения и структура современных вирусов.	Углубление знаний по данной теме	Выполнение упражнений	Ознакомление с принципами добавочной защиты операциионных систем Windows-2010, XP, Vista, и др.	[1,3,7]
Способы заражения программ.	Углубление знаний по данной теме	Выполнение упражнений	Виды, функции, способы реализации межсетевых экранов	[6]
Классификация антивирусных программ.	Углубление знаний по данной теме	Выполнение упражнений	Принципы и методология проектирования оптимальных систем защиты.	[1,8,9]
Административный уровень защиты информации	Углубление знаний по данной теме	Выполнение упражнений	Перехват данных (ложные ARP-ответы, ложная загрузка программ)	[4,5]
Шифры замены.	Углубление знаний по данной теме	Выполнение упражнений	Имперсонация (имперсонация без обратной связи и др.).	
Шифры перестановки.	Углубление знаний по данной теме	Выполнение упражнений	Провести анализ сетевых топологий и обоснование архитектуры сети, необходимой для организации распределенных вычислений	[2,4,7]
Шифрование методом гаммирования и с помощью аналитического преобразования.	Углубление знаний по данной теме	Выполнение упражнений	Несанкционированная подмена данных (туннелирование, атака мелкими обрывками, др.)	[3,5,7]
Стандарты шифрования.	Углубление	Выполнение	Отказ от работы	[1,9,10]

	знаний по данной теме	упражнений	(DoS). Разделение всех DoS атак на группы.	
Защита ПК от несанкционированного доступа.	Углубление знаний по данной теме	Выполнение упражнений	Рассмотреть межсетевые экраны фирмы Cisco Systems, NORTEL и других по типичным решениям и частям.	[10]
Программные средства защиты информации.	Углубление знаний по данной теме	Выполнение упражнений	Рассмотреть IDS компаний D-Link, Cisco Systems и других по типичным решениям и частям.	[5,7]
Управление доступом.	Углубление знаний по данной теме	Выполнение упражнений	Описать аппаратную реализацию сервера	[3,7]
Защита информации от копирования.	Углубление знаний по данной теме	Выполнение упражнений	Системы предотвра-щения атак (IPS) компаний McAfee, NetScreen, ISS.	[8,10]
Акустические каналы утечки информации. Воздушные, вибрационные, электроакустические, оптико-электронные и параметрические каналы.	Углубление знаний по данной теме	Выполнение упражнений	Ограничение доступа	[1,10]

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% в соответствии с таблицей.

Оценка по буквенной системе	Цифровые эквиваленты буквенной оценки	Процентное содержание усвоенных знаний	Оценка по традиционной системе
A A-	4,0 3,67	95-100 90-94	Отлично
B+ B B-	3,33 3,0 2,67	85-89 80-84 75-79	Хорошо
C+ C	2,33 2,0	70-74 65-69	Удовлетворительно

C- D+ D-	1,67 1,33 1,0	60-64 55-59 50-54	
F	0	0-49	Неудовлетворительно

Оценка «A» (отлично) выставляется в том случае, если магистрант в течение семестра показал отличные знания по всем программным вопросам дисциплины, а также по темам самостоятельной работы, регулярно сдавал рубежные задания, проявлял самостоятельность в изучении теоретических и прикладных вопросов по основной программе изучаемой дисциплины, а также по внепрограммным вопросам.

Оценка «A-» (отлично) предполагает отличное знание основных законов и процессов, понятий, способность к обобщению теоретических вопросов дисциплины, регулярную сдачу рубежных заданий по аудиторной и самостоятельной работе.

Оценка «B+» (хорошо) выставляется в том случае, если магистрант показал хорошие и отличные знания по вопросам дисциплины, регулярно сдавал семестровые задания в основном на «отлично» и некоторые на «хорошо».

Оценка «B» (хорошо) выставляется в том случае, если магистрант показал хорошие знания по вопросам, раскрывающим основное содержание конкретной темы дисциплины, а также темы самостоятельной работы, регулярно сдавал семестровые задания на «хорошо» и «отлично».

Оценка «B-»(хорошо) выставляется магистранту в том случае, если он хорошо ориентируется в теоретических и прикладных вопросах дисциплины как по аудиторным, так и по темам СРМ, но нерегулярно сдавал в семестре рубежные задания и имел случаи пересдачи семестровых заданий по дисциплине.

Оценка «C+» (удовлетворительно) выставляется магистранту в том случае, если он владеет вопросами понятийного характера по всем видам аудиторных занятий и СРМ, может раскрыть содержание отдельных модулей дисциплины, сдает на «хорошо» и «удовлетворительно» семестровые задания.

Оценка «C» (удовлетворительно) выставляется магистранту в том случае, если он владеет вопросами понятийного характера по всем видам аудиторных занятий и СРМ, может раскрыть содержание отдельных модулей дисциплины, сдает на «удовлетворительно» семестровые задания.

Оценка «C-» (удовлетворительно) выставляется магистранту в том случае, если студент в течение семестра регулярно сдавал семестровые задания, но по вопросам аудиторных занятий и СРМ владеет только общими понятиями и может объяснить только отдельные закономерности и их понимание в рамках конкретной темы.

Оценка «D+» (удовлетворительно) выставляется магистранту в том случае, если он нерегулярно сдавал семестровые задания, по вопросам аудиторных занятий и СРМ владеет только общими понятиями и может объяснить только отдельные закономерности и их понимание в рамках конкретной темы.

Оценка «D» (удовлетворительно) выставляется магистранту в том случае, если он нерегулярно сдавал семестровые задания, по вопросам аудиторных занятий и СРМ владеет минимальным объемом знаний, а также допускал пропуски занятий.

Оценка «F» (неудовлетворительно) выставляется тогда, когда магистрант практически не владеет минимальным теоретическим и практическим материалом аудиторных занятий и СРМ по дисциплине, нерегулярно посещает занятия и не сдает вовремя семестровые задания.

Рубежный контроль проводится на 7, 14-й неделях обучения и складывается, исходя из следующих видов контроля:

Вид контроля	%-ое содержание	Академический период обучения, неделя															Итого, %
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Посещаемость	0,7	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	10,5
Защита лаб.работ	3,5		*		*		*		*		*		*		*		24,5
Контр.задания к СРМ по лекциям	0,5	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	7,5
Упражнения к темам СРМП	0,5	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	7,5
Теорет. модуль	5							*							*		10
КП	20																20
Экзамен	20																20
Всего по аттест.								30							30		60
Итого																	100

Политика и процедуры

При изучении дисциплины «Сетевая безопасность» необходимо соблюдать следующие правила:

1. Не опаздывать на занятия.

2. В обязанности студента входит посещение всех видов занятий, при пропуске занятия в случае болезни предоставлять мед. справку, в других случаях – объяснительную записку за подписью декана.

3. Пропущенные лабораторные занятия отрабатывать в указанное преподавателем время.

4. Сдавать все виды контроля, согласно календарному графику учебного процесса.

5. Быть терпимыми, открытыми, откровенными и доброжелательными к сокурсникам и преподавателям.

Учебно-методическая обеспеченность дисциплины

Ф.И.О автора	Наименование учебно-методической литературы	Издательство, год издания	Количество экземпляров	
			В библиотеке	на кафедре
Основная литература				
Галатенко В.А.	Основы информационной безопасности.	Изд-во «Финансы и статистика», 2010	2	1
Зегжда Д.П., Ивашко А.М.	Основы безопасности информационных систем	Изд-во «Горячая линия – Телеком», 2012	1	
Касперский Е.	Компьютерные вирусы в М8-ОО8	Изд-во «Эдель-Ренессанс», 2010	1	
Партыка Т.Л., Попов И.И.	Информационная безопасность.	М.: ФОРУМ: ИНФРА – М, 2013	4	
Дополнительная литература				
Аскеров Т.М.	Защита информации и информационная безопасность	М.: Рос. экон. академия, 2012	1	
Анин Б.Ю.	Защита компьютерной информации	СПб.: БХВ - Санкт-Петербург, 2011	1	
Герасименко В.А., Машок А.А.	Основы защиты информации	М.: ООО «Инкомбук», 2013	3	1
Зима В.М., Молдовян А.А., Молдовян Н.А.	Защита компьютерных ресурсов от несанкционированных действий пользователей	СПб., 2010	3	
Петров В.А., Пискарев А.С., Шеин А.В	Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах	М.: МИФИ, 2010	1	

Ухлинов Л.М.	Международные стандарты в области обеспечения безопасности данных в сетях ЭВМ. Состояние и направление развития.	М.: Электросвязь, 2010	2	
Щербаков А.	Разрушающие программные воздействия	М.: ЭДЭЛЬ, 2013	1	

График выполнения и сдачи заданий по дисциплине

Вид контроля	Цель и содержание задания	Рекомендуемая литература	Продолжительность выполнения	Форма контроля	Срок сдачи
Посещаемость лекций	Усвоение материала по темам лекций	[1..11], конспекты лекций	15 ч	Текущий	На каждой лекции
Защита лабораторных работ №№1-7	Усвоение материала по темам лабораторных работ, приобретение практических навыков	МУ к выполнению лабораторных работ	15 ч	Текущий	На 2,4,6,8,10, 12,14 неделях
Контрольные задания к СРС по лекциям	Проверка усвоения материала лекций дисциплины	[1..11], конспекты лекций	60 ч	Текущий	Еженедельно
Упражнения к темам СРСП	Углубление знаний по темам лекций	Согласно тематике СРСП	30 ч	Текущий	Еженедельно
Теоретический модуль №№1, 2	Проверка знаний по темам лекций №1-9	Весь перечень основной и дополнительной литературы	1 контактный час	Рубежный	На 7, 14 неделях
Экзамен	Проверка усвоения материала дисциплины	Весь перечень основной и дополнительной литературы	2 контактных часа	Итоговый	В период сессии

Вопросы для самоконтроля:

1. В чем заключаются жизненно важные интересы в информационной сфере?
2. Назовите актуальные причины, обуславливающие необходимость защиты информации.
3. Укажите основную цель создания системы компьютерной безопасности.
4. Назовите основные защищаемые объекты.
5. Что такое информационная безопасность, каковы ее аспекты?
6. Что такое защита информации?

7. Что относится к поддерживающей инфраструктуре информационной системы?
8. Перечислите задачи защиты информации.
9. Что такое государственная тайна?
10. Что такое коммерческая тайна?
11. Что такое профессиональная тайна?
12. Что такое служебная тайна?
13. Назовите основные защищаемые объекты.
14. Дайте определение понятиям класс и объект.
15. Перечислите и охарактеризуйте свойства объекта.
16. Что называется гранями объекта? Приведите пример.
17. Назовите грани информационной безопасности.
18. Как можно рассматривать защищаемую ИС, варьируя уровень детализации?
19. Что понимается под угрозой?
20. В чем разница между угрозой и атакой?
21. Приведите примеры злоумышленников?
22. Что называется окном опасности?
23. Можно ли в информационной системе полностью ликвидировать окно опасности?
24. Перечислите виды угроз. На какой аспект информационной безопасности они направлены?
25. Приведите прим случайных и преднамеренных угроз.
26. Приведите пример угроз доступности.
27. Приведите пример угроз конфиденциальности.
28. Приведите пример угроз целостности.
29. Какие направления мер по защите информации вам известны?
30. Перечислите основные программно – технические средства защиты компьютерной информации.
31. Назовите средства защиты от сбоев в электропитании.
32. Назовите средства защиты от сбоев в работе процессоров и устройств хранения информации.
33. Назовите средства защиты от утечек информации за счет формирования электромагнитных излучений.
34. Что относится к программным средствам защиты информации?
35. Что понимается под административным уровнем защиты информации?
36. Что такое политика безопасности?
37. Дайте характеристику уровням политики безопасности.
38. Что подразумевает программы безопасности?
39. Что является основой программы безопасности?
40. Дайте характеристику уровням программы безопасности.
41. Каковы отличительные особенности ПК как объекта защиты?
42. Каковы потенциальные угрозы информации, обрабатываемой ПК?
43. Перечислите возможные методы взлома на уровне систем управления базами данных. Примеры.
44. Перечислите возможные методы взлома на уровне операционных систем.
45. Перечислите возможные методы взлома на уровне сетевого программного обеспечения.
46. Укажите способы защиты информации в сети.
47. Укажите возможные каналы несанкционированного доступа к информации в ПК.
48. Какие существуют программно – аппаратные средства разграничения доступа к информации в ПК?
49. Что означает разграничение доступа к информации?
50. Какова схема распределения средств защиты по возможным каналам несанкционированного доступа к ПК?

51. Что понимается под опознаванием пользователя?
52. Перечислите и охарактеризуйте способы опознавания пользователей.
53. В чем заключается суть идентификации и установления подлинности документов?
54. Что подразумевает криптографическое закрытие информации?
55. Что понимается под регистрацией обращений к системе?
56. Что понимается под идентификацией и аутентификацией пользователя в системе?
57. Приведите примеры идентификатора пользователя.
58. Что понимается под парольной аутентификацией? В чем ее преимущества и недостатки?
59. Объясните понятие «одноразовый пароль».
60. Опишите механизм работы сервера аутентификации Kerberos.
61. Объясните механизм биометрической аутентификации.
62. В чем разница между динамическими и статическими биометрическими характеристиками объекта?
63. Приведите пример физиологических и поведенческих характеристик пользователя.
64. Опишите механизм идентификации и аутентификации в ОС Windows
65. Что понимается под протоколированием?
66. В чем разница между аудитом и активным аудитом?
67. Перечислите и охарактеризуйте функции протоколирования и аудита.
68. Каким образом можно обнаружить подозрительную активность и нетипичное поведение пользователя? Пример.
69. Что означает для ПК «система порогов»?
70. Перечислите основные компоненты активного аудита.
71. Дайте характеристику компонентам активного аудита.

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ ДЛЯ СТУДЕНТА (SYLLABUS)

Дисциплина **SB 4222** Сетевая безопасность

Модуль **SBI 25** Сетевая безопасность и Интернет

Специальность 5В070400 – «Вычислительная техника и программное обеспечение»

Факультет Информационные технологии

Кафедра Информационно-вычислительные системы

Гос.изд.лиц. № 50 от 31.03.2004. Подписано в печать ___.___.15г.
Формат 60х90/16 Усл.печ.л. 1,1 Тираж Цена договорная

Издательство Карагандинского государственного технического университета
100027, Караганда, б.Мира, 56