Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра автоматики

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность информационных ресурсов

Образовательная программа: 27.03.04 Управление в технических системах, профиль: Автоматика и управление

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**7**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	81
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	36
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	7
10	Самостоятельная работа, час.	63
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 27.03.04 Управление в технических системах

ФГОС введен в действие приказом №1171 от 20.10.2015 г. , дата утверждения: 12.11.2015 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 27.03.04 Управление в технических системах

Рабочая программа обсуждена на заседании кафедры

АВТ, протокол заседания кафедры №10/1 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Басыня Е. А.

Заведующий кафедрой:

доцент, д.т.н. Жмудь В. А.

Ответственный за образовательную программу:

заведующий кафедрой Жмудь В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.9 способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности; *в части следующих результатов обучения*:**
з2. знать функции сканеров уязвимостей и принципы работы межсетевых экранов
з3. знать об уязвимости популярных операционных систем и системного ПО
з4. знать требования стандартов по обеспечению информационной безопасности
у2. уметь применять системный подход к обеспечению информационной безопасности систем и сетей в различных сферах деятельности
у5. уметь проводить анализ безопасности серверов и сетевых служб
у6. уметь применять сканеры уязвимостей и программные и аппаратные межсетевые экраны
у7. уметь планировать проведение анализа безопасности информационных ресурсов
***Компетенция ФГОС*: ПК.6 способность производить расчеты и проектирование отдельных блоков и устройств систем автоматизации и управления и выбирать стандартные средства автоматики, измерительной и вычислительной техники для проектирования систем автоматизации и управления в соответствии с техническим заданием; *в части следующих результатов обучения*:**
з6. знать организацию, архитектуру и возможности компьютерных сетей

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Безопасность информационных ресурсов	
ОПК.9.з2 знать функции сканеров уязвимостей и принципы работы межсетевых экранов	
1.знать функции сканеров уязвимостей и принципы работы межсетевых экранов	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.з3 знать об уязвимости популярных операционных систем и системного ПО	
2.знать об уязвимости популярных операционных систем и системного ПО	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.з4 знать требования стандартов по обеспечению информационной безопасности	
3.знать требования стандартов по обеспечению информационной безопасности	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.у2 уметь применять системный подход к обеспечению информационной безопасности систем и сетей в различных сферах деятельности	
4.уметь применять системный подход к обеспечению информационной безопасности систем и сетей в различных сферах деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.у5 уметь проводить анализ безопасности серверов и сетевых служб	
5.уметь проводить анализ безопасности серверов и сетевых служб	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.у6 уметь применять сканеры уязвимостей и программные и аппаратные межсетевые экраны	
6.уметь применять сканеры уязвимостей и программные и аппаратные межсетевые экраны	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.у7 уметь планировать проведение анализа безопасности информационных ресурсов	

7.уметь планировать проведение анализа безопасности информационных ресурсов	Лекции; Лабораторные работы; Самостоятельная работа
ПК.6.з6 знать организацию, архитектуру и возможности компьютерных сетей	
8.знать организацию, архитектуру и возможности компьютерных сетей	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 7			
Дидактическая единица: История проблемы. Методы взлома			
1. История проблемы, эволюция способов взлома и методов защиты.	0	4	1, 2, 4
2. Принципы анализа системы с позиции взломщика	0	4	3, 4, 5
3. Влияние человеческого фактора на обеспечение информационной безопасности	0	4	2, 3, 4, 6
4. Методы социальной инженерии.	0	4	2, 3, 5
Дидактическая единица: Требования стандартов по обеспечению информационной безопасности			
5. Требования государственных стандартов.	0	4	3, 4
6. Требования международных стандартов	0	4	2, 6, 7
7. Функции сканеров уязвимостей	0	4	1, 2, 4, 5
Дидактическая единица: Принципы работы межсетевых экранов			
8. Различия программных и аппаратных межсетевых экранов.	0	4	3, 4, 5, 7
9. Принципы работы межсетевых экранов.	0	4	5, 6, 7, 8

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: История проблемы. Методы взлома				
1. Способы взлома	6	6	1, 2, 4, 5	
2. Методов защиты.	6	6	3, 6, 7	
Дидактическая единица: Требования стандартов по обеспечению информационной безопасности				
3. Уязвимости популярных операционных систем	6	6	2, 3, 4, 5	
4. Уязвимости системного ПО.	0	6	2, 3, 4, 5	
Дидактическая единица: Принципы работы межсетевых экранов				

5. Программные межсетевые экраны популярных ОС	0	6	2, 3, 4, 5, 6	
6. Аппаратные межсетевые экраны, их особенности.	0	6	3, 4, 5, 6, 8	

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	РГЗ	1, 2, 4	4	4
: Безопасность информационных ресурсов : методические указания к лабораторным работам по направлению 27.03.04 "Управление в технических системах" дневной формы обучения / Новосиб. гос. техн. ун-т ; [сост.: Е. А. Басыня, Г. А. Французова, А. В. Гунько]. - Новосибирск, 2016. - 28, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000228040				
2	Подготовка к занятиям	1, 2, 3, 4, 5, 6, 7, 8	15	0
: Безопасность информационных ресурсов : методические указания к лабораторным работам по направлению 27.03.04 "Управление в технических системах" дневной формы обучения / Новосиб. гос. техн. ун-т ; [сост.: Е. А. Басыня, Г. А. Французова, А. В. Гунько]. - Новосибирск, 2016. - 28, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000228040				
3	Подготовка к аттестации	1, 2, 3, 4, 5, 6, 7	19	3
, подробная информация приведена в приложении №3 : Безопасность информационных ресурсов : методические указания к лабораторным работам по направлению 27.03.04 "Управление в технических системах" дневной формы обучения / Новосиб. гос. техн. ун-т ; [сост.: Е. А. Басыня, Г. А. Французова, А. В. Гунько]. - Новосибирск, 2016. - 28, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000228040				
4	Подготовка к аттестации	1, 2, 3, 4, 5, 6, 7	25	0
: Безопасность информационных ресурсов : методические указания к лабораторным работам по направлению 27.03.04 "Управление в технических системах" дневной формы обучения / Новосиб. гос. техн. ун-т ; [сост.: Е. А. Басыня, Г. А. Французова, А. В. Гунько]. - Новосибирск, 2016. - 28, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000228040				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Личный типовой сайт; Среда электронного обучения НГТУ
Консультирование	e-mail; Личный типовой сайт
Контроль	e-mail
Размещение учебных материалов	e-mail; Личный типовой сайт; Среда электронного обучения НГТУ

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 7		
Лабораторная:	25	40
РГЗ:	10	20
Контролирующие материалы - тесты		
Зачет:	15	40

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Зачет
ОПК.9	з2. знать функции сканеров уязвимостей и принципы работы межсетевых экранов	+	+
	з3. знать об уязвимости популярных операционных систем и системного ПО	+	+
	з4. знать требования стандартов по обеспечению информационной безопасности		+
	у2. уметь применять системный подход к обеспечению информационной безопасности систем и сетей в различных сферах деятельности		+
	у5. уметь проводить анализ безопасности серверов и сетевых служб		+
	у6. уметь применять сканеры уязвимостей и программные и аппаратные межсетевые экраны		+
	у7. уметь планировать проведение анализа безопасности информационных ресурсов		+
ПК.6	з6. знать организацию, архитектуру и возможности компьютерных сетей		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : [учебное пособие для вузов по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем"] / В. Олифер, Н. Олифер. - СПб. [и др.], 2012. - 943 с. : ил.

2. Громов Ю. Ю. Информационная безопасность : учеб / Ю. Ю. Громов. - Москва, 2014

3. Абденов А. Ж. Методика оценки риска для информационных систем на основе экспертных оценок : учебное пособие / А. Ж. Абденов, С. А. Белкин, Р. Н. Заркумова-Райхель ; Новосиб. гос. техн. ун-т. - Новосибирск, 2014. - 69, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000213163

4. Басыня Е. А. Сетевая информационная безопасность и анонимизация : учебное пособие / Е. А. Басыня ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 74, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000233806

Дополнительная литература

1. ГОСТ Р 52633.4-2011. Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа / Федер. агентство по техн. регулированию и метрологии. - Москва, 2012. - IV, 41, [1] с. : табл.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Безопасность информационных ресурсов : методические указания к лабораторным работам по направлению 27.03.04 "Управление в технических системах" дневной формы обучения / Новосиб. гос. техн. ун-т ; [сост.: Е. А. Басыня, Г. А. Французова, А. В. Гунько]. - Новосибирск, 2016. - 28, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000228040

8.2 Специализированное программное обеспечение

1 Операционные системы семества LINUX

9. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Компьютеры объединены в локальную сеть с выходом в Internet

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра автоматики

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность информационных ресурсов

Образовательная программа: 27.03.04 Управление в технических системах, профиль: Автоматика и управление

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Безопасность информационных ресурсов приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК.9 способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности	з2. знать функции сканеров уязвимостей и принципы работы межсетевых экранов	История проблемы, эволюция способов взлома и методов защиты. Способы взлома Функции сканеров уязвимостей	РГЗ	Зачет, вопросы 1-7
ОПК.9	з3. знать об уязвимости популярных операционных систем и системного ПО	Влияние человеческого фактора на обеспечение информационной безопасности История проблемы, эволюция способов взлома и методов защиты. Методы социальной инженерии. Программные межсетевые экраны популярных ОС Способы взлома Требования международных стандартов Уязвимости популярных операционных систем Уязвимости системного ПО. Функции сканеров уязвимостей	РГЗ	Зачет, вопросы 8-13
ОПК.9	з4. знать требования стандартов по обеспечению информационной безопасности	Аппаратные межсетевые экраны, их особенности. Влияние человеческого фактора на обеспечение информационной безопасности Методов защиты. Методы социальной инженерии. Принципы анализа системы с позиции взломщика Программные межсетевые экраны популярных ОС Различия программных и аппаратных межсетевых экранов. Требования государственных стандартов. Уязвимости популярных операционных систем Уязвимости системного ПО.		Зачет, вопросы 14-20
ОПК.9	у2. уметь применять системный подход к обеспечению информационной безопасности	Аппаратные межсетевые экраны, их особенности. Влияние человеческого фактора на обеспечение информационной		Зачет, вопросы 21-26

	систем и сетей в различных сферах деятельности	безопасности История проблемы, эволюция способов взлома и методов защиты. Принципы анализа системы с позиции взломщика Программные межсетевые экраны популярных ОС Различия программных и аппаратных межсетевых экранов. Способы взлома Требования государственных стандартов. Уязвимости популярных операционных систем Уязвимости системного ПО. Функции сканеров уязвимостей		
ОПК.9	у5. уметь проводить анализ безопасности серверов и сетевых служб	Аппаратные межсетевые экраны, их особенности. Методы социальной инженерии. Принципы анализа системы с позиции взломщика Принципы работы межсетевых экранов. Программные межсетевые экраны популярных ОС Различия программных и аппаратных межсетевых экранов. Способы взлома Уязвимости популярных операционных систем Уязвимости системного ПО. Функции сканеров уязвимостей		Зачет, вопросы 27-35
ОПК.9	у6. уметь применять сканеры уязвимостей и программные и аппаратные межсетевые экраны	Аппаратные межсетевые экраны, их особенности. Влияние человеческого фактора на обеспечение информационной безопасности Методов защиты. Принципы работы межсетевых экранов. Программные межсетевые экраны популярных ОС Требования международных стандартов		Зачет, вопросы 36-40
ОПК.9	у7. уметь планировать проведение анализа безопасности информационных ресурсов	Методов защиты. Принципы работы межсетевых экранов. Различия программных и аппаратных межсетевых экранов. Требования международных стандартов		Зачет, вопросы 41-45
ПК.6/ПК способность производить расчеты и проектирование отдельных блоков и устройств систем автоматизации и управления и выбирать стандартные средства автоматики, измерительной и вычислительной	з6. знать организацию, архитектуру и возможности компьютерных сетей	Принципы работы межсетевых экранов.		Зачет, вопросы 46-51

техники для проектирования систем автоматизации и управления в соответствии с техническим заданием				

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 7 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ОПК.9, ПК.6/ПК.

Зачет проводится в письменной форме, по билетам.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 7 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (РГЗ). Требования к выполнению РГЗ, состав и правила оценки сформулированы в паспорте РГЗ.

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.9, ПК.6/ПК, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автоматики

Паспорт зачета

по дисциплине «Безопасность информационных ресурсов», 7 семестр

1. Методика оценки

Зачет проводится в письменной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-25, второй вопрос из диапазона вопросов 26-51 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Безопасность информационных ресурсов»

---

1. Вопрос 1. Алгоритмы и методы работы IDS/IPS
2. Вопрос 2. Тестирование на проникновение: технические и правовые аспекты.
3. Задача. Продемонстрируйте на практике навыки работы с пакетным фильтром и трассировщиком соединений на примере настройки DMZ, SNAT и DNAT

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки

- Ответ на билет для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет менее 10 *баллов.*
- Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет от 11 до 20 *баллов.*
- Ответ на билет для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет от 21 до 30 *баллов.*
- Ответ на билет (тест) для зачета билет засчитывается на **продвинутом** уровне, если

студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет от 31 до 40 *баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 15 баллов (из 40 возможных).

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине «**Безопасность информационных ресурсов**»**

1) Алгоритмы и методы работы IDS/IPS.
2) Основные положения указа Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы".
3) Принцип работы SSL. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.
4) Уязвимости стека протоколов TCP/IP.
5) Основные положения указа Президента Российской Федерации от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
6) Принцип работы TLS. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.
7) Уязвимости ОС семейства Windows.
8) Технические стандарты и спецификации в области информационной безопасности.
9) Принцип работы SSH. Конфигурирование клиента и сервера с обеспечением информационной безопасности.
10) Уязвимости ОС семейства Linux.
11) Международные документы/регламенты в области информационной безопасности.
12) Принцип работы RDP. Конфигурирование клиента и терминального сервера WS08/12/16 с обеспечением информационной безопасности.
13) Методы и средства анализа уязвимостей систем и сетей.
14) Kali Linux и Tails: функциональное назначение, принцип работы, технические нюансы использования.
15) X509. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.
16) Уязвимости системного и прикладного программного обеспечения, инструменты и средства защиты.
17) Маршрутизация сетевого трафика на базе стека протоколов TCP/IP. Уязвимости и средства их устранения.
18) Многопользовательский режим работы SFTP. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.
19) Межсетевые экраны (программные и аппаратно-программные). UTM и NGFW решения.
20) Правовые и технические аспекты работы с персональными данными.
21) Многопользовательский режим работы FTPS. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.

22) Интеграция SIEM и IDS/IPS.

23) Лицензирование деятельности и сертификация продуктов в сфере информационной безопасности.

24) Технологии виртуальных защищенных каналов связи. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.

25) Web-application firewall: функциональное назначение и принцип работы.

26) Тестирование на проникновение: технические и правовые аспекты.

27) Продемонстрируйте на практике навыки работы с настройкой любой IDS/IPS от зондирования информационного ресурса.

28) Оверлейные системы и сети: алгоритмы и методы продвижения информационных потоков, маршрутизация трафика.

29) Технологии проксирования: функциональное назначение и принцип работы.

30) Продемонстрируйте на практике навыки работы с пакетным фильтром и трассировщиком соединений на примере настройки DMZ, SNAT и DNAT.

31) Безопасность виртуальных инфраструктур (на примере гипервизора / паравиртуализатора).

32) Алгоритмы обхода систем защиты (на примере IDS/IPS).

33) Принцип работы DES, 3DES, AES. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.

34) Комплексные меры обеспечения безопасности информационных ресурсов. Системы обнаружения и предотвращения вторжений.

35) Перечень основных ГОСТов РФ в области криптографии.

36) Принцип работы PGP, OTR. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.

37) Технология виртуальных защищенных каналов связи.

38) SOCKS5: функциональное назначение и принцип работы.

39) Принцип работы XMPP. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.

40) Влияние структуры корпоративной вычислительной сети на ее защищенность от сетевых атак.

41) SELinux: функциональное назначение и принцип работы.

42) Принцип работы OpenVPN, IPsec. Установка и конфигурирование любого серверного решения (отражающего вашу квалификацию) на базе ОС семейства Linux с использованием данной технологии.

43) Программные криптографические механизмы защиты информации.

44) Алгоритм простукивания портов.

45) Продемонстрируйте на практике навыки работы с пакетным фильтром и трассировщиком соединений на примере настройки MASQUERADE и mangle.

46) Шифрование системного раздела: программного обеспечение, алгоритмы и протоколы.

47) Уязвимости технологий DHCP и DNS, методы их устранения.

48) Продемонстрируйте на практике навыки работы с обеспечением информационной безопасности Web-сервера.

49) Резервное копирование файлов, БД, ОС: принципы, протоколы, алгоритмы, программные решения.

50) Симметричное и ассиметричное шифрование. Какая максимальная битность люча разрешена ФСБ/ФСТЭК на территории РФ для различных сфер применения?

51) Продемонстрируйте на практике навыки работы с настройкой любой IDS/IPS от сканирования информационного ресурса.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автоматики

Паспорт
расчетно-графического задания (работы)

по дисциплине «Безопасность информационных ресурсов», 7 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны спроектировать корпоративную вычислительную сеть, состоящую из 100 хостов. Установить и сконфигурировать головной шлюз на базе серверной операционной системы Windows или Unix/Linux. При выполнении расчетно-графического задания (работы) студенты должны провести анализ объекта КВС, выбрать и обосновать диагностические признаки и параметры, разработать алгоритмы диагностирования, выбрать аппаратные средства.

Содержание отчета

1. Цель работы.
2. Техническое задание.
3. Сравнительный анализ существующих решений.
4. Установка и конфигурирование серверного решения.
5. Реализация комплекса мер по обеспечению ИБ.
6. Заключение.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ, отсутствует анализ объекта, диагностические признаки не обоснованы, аппаратные средства не выбраны или не соответствуют современным требованиям, оценка составляет менее 10 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, аппаратные средства не соответствуют современным требованиям, оценка составляет от 10 до 13 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны ,но не оптимизированы, аппаратные средства выбраны без достаточного обоснования, оценка составляет от 14 до 16 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны и оптимизированы, выбор аппаратных средств обоснован, оценка составляет от 17 до 20 баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ

Спроектировать корпоративную вычислительную сеть, состоящую из 100 хостов. Установить и сконфигурировать головной шлюз на базе серверной операционной системы Windows или Unix/Linux. Провести анализ объекта КВС, выбрать и обосновать диагностические признаки и параметры, разработать алгоритмы диагностирования, выбрать аппаратные средства.