Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
_____ Н.Г. Кузнецов
«01» июня 2018г.

Рабочая программа дисциплины

Защита информационных процессов и систем

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
Недель	17,3			
Вид занятий	УП	РПД	УП	РПД
Лекции	36	36	36	36
Лабораторные	36	36	36	36
В том числе инт.	14	14	14	14
Итого ауд.	72	72	72	72
Контактная	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): д.т.н., профессор, Соколов С.В. _____ 11.05.18

Зав. кафедрой: Тищенко Е.Н. _____ 11.05.18

Методическим советом направления: к.ф.-м.н., Карасев Д.Н. _____ 16.05.18

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.18

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.18

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: Тищенко Е.Н. _____

Программу составил(и): д.т.н., профессор, Соколов С.В. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель курса: изучить теоретические основы информационной безопасности (ИБ) и методологические нормы системного обеспечения защиты информационных процессов в компьютерных системах.
1.2	Задачи курса: раскрытие понятийного аппарата в области ИБ и ЗИ в компьютерных системах; раскрытие содержательных базовых положений; раскрытие современной доктрины ИБ; определение целей и принципов ЗИ в компьютерных системах; обновление факторов, влияющих на ЗИ; установление угроз информации в компьютерных системах; раскрытие направлений, видов, методов и особенностей деятельности злоумышленников в компьютерной сети и при наличии изолированного компьютера; раскрытие назначения, сущности и структуры системы ЗИ в компьютерных системах, системных вопросов защиты программ и данных; определение требований к программной и программно-аппаратной реализации средств ЗИ в компьютерных системах и к защите АСУ от несанкционированного доступа (НСД).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного освоения являются навыки, знания и умения, полученные в результате освоения дисциплин:
2.1.2	Информационная безопасность в системах электронной коммерции
2.1.3	Методы атакующего воздействия на информационные ресурсы
2.1.4	Средства и методы защиты хранилищ и баз данных
2.1.5	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Администрирование защищенных информационных систем
2.2.2	Криптографические методы защиты информации
2.2.3	Организация и управление службой защиты информации
2.2.4	Системы защиты информации в ведущих зарубежных странах
2.2.5	Специальные методы исследования аппаратных средств информационных систем
2.2.6	Техническая защита информации
2.2.7	Технология сбора и анализа информации
2.2.8	Управление информационной безопасностью

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
Знать:
Методы применения информационных технологий для поиска и обработки информации на базовом уровне
Уметь:
Применять методы применения информационных технологий для поиска и обработки информации на базовом уровне
Владеть:
Методами применения информационных технологий для поиска и обработки информации на базовом уровне
ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
Знать:
Методы определения угроз информационной безопасности и возможные пути их реализации на базовом уровне
Уметь:
Применять методы определения угроз информационной безопасности и возможные пути их реализации на базовом уровне
Владеть:
Методами определения угроз информационной безопасности и возможные пути их реализации на базовом уровне
ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
Знать:
методы участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты
Уметь:

применять методы участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты
Владеть:
методами участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Интер акт.	Примечание
	Раздел 1. Основные составляющие и угрозы информационной безопасности (ИБ).						
1.1	Введение: сущность и понятие ИБ; значение ИБ и ее место в системе национальной безопасности /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	2	
1.2	Основные определения: основные составляющие ИБ, основные принципы обеспечения ИБ. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
1.3	Угрозы информационной безопасности: основные определения и классификация угроз, основные угрозы доступности. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	2	
1.4	Защита баз данных: создание SQL – сервера с использованием пакета Firebird /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	2	
1.5	Управление защитой баз данных: управление SQL – сервером с использованием пакета Firebird /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
1.6	Особенности построений информационной безопасности: анализ угроз основным составляющим ИБ. /Ср/	6	8	ОПК-4 ОПК-7 ПК-4	Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 2. Анализ целей и средств злоумышленников в компьютерных сетях						
2.1	Удаленные сетевые атаки: классификация категорий хакеров (злоумышленников) и их целей. Организационно-коммуникативные средства НСД в компьютерную систему. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
2.2	Защита от несанкционированного доступа: средства НСД в компьютерную систему: технические, программные. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	2	
2.3	Защита сетевого взаимодействия: основные сведения об угрозах сетевого взаимодействия; анализ уязвимости информационных систем (ИС). /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
2.4	Сетевые атаки: классификация сетевых атак и анализ особенностей их организации. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
2.5	Системы контроля доступа: управление правами доступа /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	2	
2.6	Системы управления доступом: управление правами доступа в ЛВС /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	

2.7	Защита локальной вычислительной сети: неавторизованный доступ к ЛВС. НСД к ресурсам ЛВС, раскрытие и неавторизованная модификация данных и программ. /Ср/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 3. Защита операционных систем: специфика безопасности локальных вычислительных сетей (ЛВС) и информационных систем.						
3.1	Защита локальной вычислительной сети от модификации: неавторизованный доступ к ЛВС, НСД к ресурсам ЛВС, раскрытие и неавторизованная модификация данных и программ. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.2 Л2.1 Л2.2 Л3.1 Э1	2	
3.2	Защита трафика локальной вычислительной сети: раскрытие и подмена трафика ЛВС, разрушение функций ЛВС, ошибки в программном обеспечении, контроль удаленных вычислений. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
3.3	Резервное копирование данных: подготовка к резервному копированию базы данных /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
3.4	Деструктивные воздействия на локальную вычислительную сеть: разрушение функций ЛВС, ошибки в программном обеспечении. Контроль удаленных вычислений. /Ср/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 4. Программно-техническая защита: основные программно-технические меры защиты информационных процессов и программного обеспечения (ПО)						
4.1	Архитектурная безопасность: основные понятия программно-технического уровня ИБ, особенности ИБ современных ИС, архитектурная безопасность. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	2	
4.2	Структурная схема системы ЗИ в типовой ИС: основные функции уровней ЗИ в ИС. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
4.3	Средства собственной защиты ПО: средства защиты в составе вычислительной системы, средства защиты с запросом информации. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
4.4	Типы защиты программного обеспечения: средства активной защиты ПО, средства пассивной защиты. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
4.5	Защита СУБД: резервное копирование базы данных /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
4.6	Защита в *nix-системах: управление Unix – подобной системой. /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
4.7	Собственная защита: средства собственной защиты. /Ср/	6	8	ОПК-4 ОПК-7	Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	

	Раздел 5. Структура требований к средствам защиты: основные категории требований к программной и программно-аппаратной реализации средств защиты информации.						
5.1	Общие требования по обеспечению ИБ: требования к программно-аппаратным средствам, требования к информационным подсистемам (идентификации и аутентификации, управления доступом). /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
5.2	Общие требования к информационным подсистемам (протоколирования, аудита и т.д.), требования к средствам управления ИБ, требования к межсетевому экрану. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
5.3	Виртуализация: установка сервера на виртуальную машину. /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
5.4	Встроенные средства защиты: средства защиты в составе вычислительной системы. /Ср/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 6. Требования к защите автоматизированных систем (АС) от НСД.						
6.1	Основные характеристики технических средств защиты от НСД: основные подсистемы ЗИ от НСД для АС (управления доступом, регистрации и учета, криптографическая, обеспечения целостности) и требования к ним. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
6.2	Анализ защищенности: показатели защищенности информации от НСД для компьютерных систем /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
6.3	Межсетевые экраны: показатели защищенности межсетевых экранов. /Лек/	6	2	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
6.4	Защита от сетевых атак: организация и отражение сетевых атак /Лаб/	6	4	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
6.5	Активная интерфейсная защита: средства защиты с запросом информации. Средства активной защиты. /Ср/	6	8	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	
6.6	/Экзамен/	6	36	ОПК-4 ОПК-7 ПК-4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

ВОПРОСЫ К ЭКЗАМЕНУ:
1.Сущность и понятие информационной безопасности (ИБ);
2.Характеристика основных составляющих ИБ;
3.Значение ИБ для субъектов информационных отношений;
4.Место ИБ в системе национальной безопасности;
5.Основные принципы обеспечения ИБ;
6.Классификация угроз ИБ;

7.Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
8.Состав и краткая характеристика основных угроз доступности;
9.Состав и краткая характеристика основных угроз целостности;
10.Состав и краткая характеристика основных угроз конфиденциальности;
11.Классификация категорий хакеров и их целей;
12.Состав и краткая характеристика организационно коммуникативных средств НСД;
13.Состав и краткая характеристика технических средств НСД;
14.Состав и краткая характеристика программных средств НСД;
15.Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
16.Классификация сетевых атак;
17.Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
18.Определение IP спуфинга и характеристика основных средств защиты от него;
19.Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;
20.Определение парольных атак и характеристика основных средств защиты от них;
21.Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;
22.Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
23.Основные методы и условия неавторизованного доступа к ЛВС;
24.Краткая характеристика основных условий НСД к ЛВС;
25.Краткая характеристика основных условий раскрытия данных ЛВС;
26.Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
27.Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
28.Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
29.Основные сервисы безопасности;
30.Основные принципы архитектурной безопасности и их краткая характеристика;
31.Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
32.Основные функции централизованного управления рисками и администрирования системы безопасности;
33.Основные функции защиты управления приложениями;
34.Основные функции защиты системы сетей;
35.Основные функции защиты конечных пользователей;
36.Классификация средств защиты программного обеспечения и характеристика их основных категорий;
37.Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
38.Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
39.Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";
40.Классификация средства защиты с запросом информации и характеристика их основных составляющих;
41.Назначение и принцип формирования паролей, шифров, сигнатур;
42.Назначение и основные принципы построения аппаратуры защиты;
43.Классификация средств активной защиты и характеристика их основных составляющих;
44.Определение и характеристика основных внутренних средств активной защиты;
45.Определение и характеристика основных внешних средств активной защиты;
46.Классификация средств пассивной защиты и характеристика их основных составляющих;
47.Назначение и основные принципы организации идентификации программ;
48.Назначение и основные принципы построения устройств контроля;
49.Общий состав требований по обеспечению ИБ;
50.Требования к программно аппаратным средствам;
51.Требования к подсистеме идентификации и аутентификации;
52.Требования к подсистеме управления доступом;
53.Требования к подсистеме протоколирования аудита;
54.Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
55.Требования к средствам обеспечения целостности;
56.Требования к средствам управления ИБ;
57.Общий состав требований к межсетевому экрану;
58.Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;
59.Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
60.Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
61.Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
62.Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика.
63.Вопросы для подготовки к экзамену.
64.Сущность и понятие информационной безопасности (ИБ);
65.Характеристика основных составляющих ИБ;
66.Значение ИБ для субъектов информационных отношений;
67.Место ИБ в системе национальной безопасности;
68.Основные принципы обеспечения ИБ;
69.Классификация угроз ИБ;
70.Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
71.Состав и краткая характеристика основных угроз доступности;
72.Состав и краткая характеристика основных угроз целостности;

73.Состав и краткая характеристика основных угроз конфиденциальности;
74.Классификация категорий хакеров и их целей;
75.Состав и краткая характеристика организационно коммуникативных средств НСД;
76.Состав и краткая характеристика технических средств НСД;
77.Состав и краткая характеристика программных средств НСД;
78.Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
79.Классификация сетевых атак;
80.Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
81.Определение IP спуфинга и характеристика основных средств защиты от него;
82.Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;
83.Определение парольных атак и характеристика основных средств защиты от них;
84.Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;
85.Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
86.Основные методы и условия неавторизованного доступа к ЛВС;
87.Краткая характеристика основных условий НСД к ЛВС;
88.Краткая характеристика основных условий раскрытия данных ЛВС;
89.Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
90.Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
91.Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
92.Основные сервисы безопасности;
93.Основные принципы архитектурной безопасности и их краткая характеристика;
94.Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
95.Основные функции централизованного управления рисками и администрирования системы безопасности;
96.Основные функции защиты управления приложениями;
97.Основные функции защиты системы сетей;
98.Основные функции защиты конечных пользователей;
99.Классификация средств защиты программного обеспечения и характеристика их основных категорий;
100.Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
101.Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
102.Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";
103.Классификация средства защиты с запросом информации и характеристика их основных составляющих;
104.Назначение и принцип формирования паролей, шифров, сигнатур;
105.Назначение и основные принципы построения аппаратуры защиты;
106.Классификация средств активной защиты и характеристика их основных составляющих;
107.Определение и характеристика основных внутренних средств активной защиты;
108. Определение и характеристика основных внешних средств активной защиты;
109.Классификация средств пассивной защиты и характеристика их основных составляющих;
110.Назначение и основные принципы организации идентификации программ;
111.Назначение и основные принципы построения устройств контроля;
112.Общий состав требований по обеспечению ИБ;
113.Требования к программно аппаратным средствам;
114.Требования к подсистеме идентификации и аутентификации;
115.Требования к подсистеме управления доступом;
116.Требования к подсистеме протоколирования аудита;
117.Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
118.Требования к средствам обеспечения целостности;
119.Требования к средствам управления ИБ;
120.Общий состав требований к межсетевому экрану;
121.Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;
122.Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
123.Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
124.Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
125.Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика.

5.2. Фонд оценочных средств для проведения текущего контроля

Структура и содержание фонда оценочных средств представлены в Приложении 1 к рабочей программе дисциплины

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Хорев П. Б.	Программно-аппаратная защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. "Информ. безопасность"	М.: ФОРУМ, 2015	25
Л1.2	Завгородний В. И.	Комплексная защита информации в компьютерных системах: Учеб. пособие	М.: Логос, 2001	49
Л1.3	Артемов А. В.	Информационная безопасность: курс лекций	Орел: МАБИВ, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Тищенко Е. Н.	Основы информационной безопасности: учеб. -метод. разраб.	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2012	10
Л2.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Тищенко Е. Н., Жилина Е. В.	Проектирование нечетких систем средствами MATLAB: практикум	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2015	63
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	Сервер компании НИП «Информзащита»/http://www.infosec.ru			
6.3. Перечень программного обеспечения				
6.3.1	Анализатор уязвимостей XSpider			
6.3.2	Анализатор уязвимостей MaxPatrol			
6.3.3	Межсетевой экран PFSense			
6.3.4	Удостоверяющий центр VipNet			
6.4 Перечень информационных справочных систем				
6.4.1	Гарант			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по усвоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины

Приложение 1
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры Информационные
технологии и защита информации
Протокол № 12 от 28.03.2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Защита информационных процессов и систем

Направление подготовки
10.03.01 Информационная безопасность

Профиль
10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Соколов С.В. профессор д.т.н. профессор
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону, 2018

Оглавление

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы 3

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания 3

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы 11

4. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы 21

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-4 способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации			
З. принципы работы, связанные с обеспечением комплексной защиты информации на основе существующих программ и методик основные угрозы информации в компьютерных системах существующие методы и средства, применяемые для контроля и защиты информации	Вопросы для текущего контроля и подготовки к экзамену Модуль 1. Сущность и понятие информационной безопасности (ИБ); Характеристика основных составляющих ИБ; Значение ИБ для субъектов информационных отношений; Место ИБ в системе национальной безопасности; Основные принципы обеспечения ИБ; Классификация угроз ИБ; Состав и краткая характеристика внутренних и внешних источников угроз ИБ; Состав и краткая характеристика основных угроз доступности; Состав и краткая характеристика основных угроз целостности; Состав и краткая характеристика основных угроз конфиденциальности; Модуль 2. Классификация категорий хакеров и их целей; Состав и краткая характеристика организационно коммуникативных средств НСД; Состав и краткая	полнота и содержательность ответа умение приводить примеры	О

	характеристика технических средств НСД; Состав и краткая характеристика программных средств НСД; Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet; Классификация сетевых атак; Определение сниффера пакетов и характеристика основных средств защиты от сниффинга; Определение IP спуфинга и характеристика основных средств защиты от него;		
У. проводить анализ материалов учреждений, организаций и предприятий отрасли с целью выработки и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну	Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них; Определение парольных атак и характеристика основных средств защиты от них; Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них; Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них; Модуль 3. Основные методы и условия неавторизованного доступа к ЛВС; Краткая характеристика основных условий НСД к ЛВС; Краткая характеристика основных условий раскрытия данных ЛВС; Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения; Краткая характеристика основных условий раскрытия и подмены трафика ЛВС; Основные угрозы ИБ ЛВС при распределенном	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

	хранении файлов и удаленных вычислениях; Основные сервисы безопасности; Основные принципы архитектурной безопасности и их краткая характеристика; Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков; Основные функции централизованного управления рисками и администрирования системы безопасности; Основные функции защиты управления приложениями; Основные функции защиты системы сетей; Основные функции защиты конечных пользователей; Модуль 4. Классификация средств защиты программного обеспечения и характеристика их основных категорий; Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих; Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;		
В. информацией о действующих нормативных и методических документах, новых схемах аппаратуры контроля, средств автоматизации контроля	Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций"; Классификация средства защиты с запросом информации и характеристика их основных составляющих; Назначение и принцип формирования паролей, шифров, сигнатур; Назначение и основные принципы построения аппаратуры защиты; Классификация средств активной защиты и характеристика их основных составляющих;	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

	Определение и характеристика основных внутренних средств активной защиты; Определение и характеристика основных внешних средств активной защиты; Классификация средств пассивной защиты и характеристика их основных составляющих; Назначение и основные принципы организации идентификации программ; Назначение и основные принципы построения устройств контроля; Модуль 5. Общий состав требований по обеспечению ИБ; Требования к программно аппаратным средствам; Требования к подсистеме идентификации и аутентификации; Требования к подсистеме управления доступом; Требования к подсистеме протоколирования аудита; Требования к подсистеме защиты повторного использования объектов и к защите критичной информации; Требования к средствам обеспечения целостности; Требования к средствам управления ИБ; Общий состав требований к межсетевому экрану; Модуль 6. Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;		
ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты			
3. системные вопросы защиты программ и данных основные категории требований к программной и программно-аппаратной реализации средств защиты информации требования к защите автоматизированных	Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД; Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для	полнота и содержательность ответа умение приводить примеры	О

систем от НСД.	защиты от НСД; Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД; Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика. Вопросы для подготовки к экзамену. Сущность и понятие информационной безопасности (ИБ); Характеристика основных составляющих ИБ; Значение ИБ для субъектов информационных отношений; Место ИБ в системе национальной безопасности; Основные принципы обеспечения ИБ; Классификация угроз ИБ; Состав и краткая характеристика внутренних и внешних источников угроз ИБ; Состав и краткая характеристика основных угроз доступности; Состав и краткая характеристика основных угроз целостности; Состав и краткая характеристика основных угроз конфиденциальности; Классификация категорий хакеров и их целей; Состав и краткая характеристика организационно коммуникативных средств НСД; Состав и краткая характеристика технических средств НСД; Состав и краткая характеристика программных средств НСД; Характеристика основных угроз ИБ при взаимодействии с Internet;		

	требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet; Классификация сетевых атак; Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;		
У. анализировать методы и средства контроля и защиты информации и разрабатывать предложения по их совершенствованию и повышению эффективности ЗИ.	Определение IP спуфинга и характеристика основных средств защиты от него; Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них; Определение парольных атак и характеристика основных средств защиты от них; Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них; Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них; Основные методы и условия неавторизованного доступа к ЛВС; Краткая характеристика основных условий НСД к ЛВС; Краткая характеристика основных условий раскрытия данных ЛВС; Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения; Краткая характеристика основных условий раскрытия и подмены трафика ЛВС; Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях; Основные сервисы безопасности; Основные принципы архитектурной безопасности и их краткая характеристика; Структурная схема	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

	системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков; Основные функции централизованного управления рисками и администрирования системы безопасности; Основные функции защиты управления приложениями; Основные функции защиты системы сетей; Основные функции защиты конечных пользователей; Классификация средств защиты программного обеспечения и характеристика их основных категорий; Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих; Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС; Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";		
В. моделях и системах защиты информации, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по ЗИ, аттестации и категорировании объектов защиты.	Классификация средства защиты с запросом информации и характеристика их основных составляющих; Назначение и принцип формирования паролей, шифров, сигнатур; Назначение и основные принципы построения аппаратуры защиты; Классификация средств активной защиты и характеристика их основных составляющих; Определение и характеристика основных внутренних средств активной защиты; Определение и характеристика основных внешних средств активной защиты; Классификация средств пассивной защиты и	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

	характеристика их основных составляющих; Назначение и основные принципы организации идентификации программ; Назначение и основные принципы построения устройств контроля; Общий состав требований по обеспечению ИБ; Требования к программно аппаратным средствам; Требования к подсистеме идентификации и аутентификации; Требования к подсистеме управления доступом; Требования к подсистеме протоколирования аудита; Требования к подсистеме защиты повторного использования объектов и к защите критичной информации; Требования к средствам обеспечения целостности; Требования к средствам управления ИБ; Общий состав требований к межсетевому экрану; Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД; Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД; Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД; Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;		
ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты			
З: методы участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению	Алгоритмы применения методов участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

информационной безопасности объекта защиты	информационной безопасности объекта защиты		
У: применять методы участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты	Последовательность применения методов участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В: методами участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты	Практические навыки применения методов участия в работах по реализации политики информационной безопасности, применения комплексного подхода к обеспечению информационной безопасности объекта защиты	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

О – опрос, ЛР- лабораторная работа

3.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

84-100 баллов (оценка «отлично»)
67-83 баллов (оценка «хорошо»)
50-66 баллов (оценка «удовлетворительно»)
0-49 баллов (оценка «неудовлетворительно»)

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

В разделе приводятся типовые варианты оценочных средств: вопросы к экзамену, задания для опроса, лабораторные работы, экзаменационный билет.

Вопросы к экзамену
по дисциплине Защита информационных процессов и систем

1) №
2) Вопросы для текущего контроля и подготовки к экзамену
3) Модуль 1.

4) Сущность и понятие информационной безопасности (ИБ);
5) Характеристика основных составляющих ИБ;
6) Значение ИБ для субъектов информационных отношений;
7) Место ИБ в системе национальной безопасности;
8) Основные принципы обеспечения ИБ;
9) Классификация угроз ИБ;
10) Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
11) Состав и краткая характеристика основных угроз доступности;
12) Состав и краткая характеристика основных угроз целостности;
13) Состав и краткая характеристика основных угроз конфиденциальности;
14) Модуль 2.
15) Классификация категорий хакеров и их целей;
16) Состав и краткая характеристика организационно коммуникативных средств НСД;
17) Состав и краткая характеристика технических средств НСД;
18) Состав и краткая характеристика программных средств НСД;
19) Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
20) Классификация сетевых атак;
21) Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
22) Определение IP спуфинга и характеристика основных средств защиты от него;
23) Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;
24) Определение парольных атак и характеристика основных средств защиты от них;
25) Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;
26) Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
27) Модуль 3.
28) Основные методы и условия неавторизованного доступа к ЛВС;
29) Краткая характеристика основных условий НСД к ЛВС;
30) Краткая характеристика основных условий раскрытия данных ЛВС;
31) Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
32) Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
33) Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
34) Основные сервисы безопасности;
35) Основные принципы архитектурной безопасности и их краткая характеристика;
36) Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
37) Основные функции централизованного управления рисками и администрирования системы безопасности;
38) Основные функции защиты управления приложениями;
39) Основные функции защиты системы сетей;
40) Основные функции защиты конечных пользователей;
41) Модуль 4.
42) Классификация средств защиты программного обеспечения и характеристика их основных категорий;
43) Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
44) Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
45) Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";
46) Классификация средства защиты с запросом информации и характеристика их основных составляющих;
47) Назначение и принцип формирования паролей, шифров, сигнатур;
48) Назначение и основные принципы построения аппаратуры защиты;

49) Классификация средств активной защиты и характеристика их основных составляющих;
50) Определение и характеристика основных внутренних средств активной защиты;
51) Определение и характеристика основных внешних средств активной защиты;
52) Классификация средств пассивной защиты и характеристика их основных составляющих;
53) Назначение и основные принципы организации идентификации программ;
54) Назначение и основные принципы построения устройств контроля;
55) Модуль 5.
56) Общий состав требований по обеспечению ИБ;
57) Требования к программно аппаратным средствам;
58) Требования к подсистеме идентификации и аутентификации;
59) Требования к подсистеме управления доступом;
60) Требования к подсистеме протоколирования аудита;
61) Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
62) Требования к средствам обеспечения целостности;
63) Требования к средствам управления ИБ;
64) Общий состав требований к межсетевому экрану;
65) Модуль 6.
66) Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;
67) Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
68) Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
69) Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
70) Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика.
71) Вопросы для подготовки к экзамену.
72) Сущность и понятие информационной безопасности (ИБ);
73) Характеристика основных составляющих ИБ;
74) Значение ИБ для субъектов информационных отношений;
75) Место ИБ в системе национальной безопасности;
76) Основные принципы обеспечения ИБ;
77) Классификация угроз ИБ;
78) Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
79) Состав и краткая характеристика основных угроз доступности;
80) Состав и краткая характеристика основных угроз целостности;
81) Состав и краткая характеристика основных угроз конфиденциальности;
82) Классификация категорий хакеров и их целей;
83) Состав и краткая характеристика организационно коммуникативных средств НСД;
84) Состав и краткая характеристика технических средств НСД;
85) Состав и краткая характеристика программных средств НСД;
86) Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
87) Классификация сетевых атак;
88) Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;
89) Определение IP спуфинга и характеристика основных средств защиты от него;
90) Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;
91) Определение парольных атак и характеристика основных средств защиты от них;
92) Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;
93) Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
94) Основные методы и условия неавторизованного доступа к ЛВС;
95) Краткая характеристика основных условий НСД к ЛВС;

96) Краткая характеристика основных условий раскрытия данных ЛВС;
97) Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;
98) Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;
99) Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;
100) Основные сервисы безопасности;
101) Основные принципы архитектурной безопасности и их краткая характеристика;
102) Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;
103) Основные функции централизованного управления рисками и администрирования системы безопасности;
104) Основные функции защиты управления приложениями;
105) Основные функции защиты системы сетей;
106) Основные функции защиты конечных пользователей;
107) Классификация средств защиты программного обеспечения и характеристика их основных категорий;
108) Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;
109) Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;
110) Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";
111) Классификация средства защиты с запросом информации и характеристика их основных составляющих;
112) Назначение и принцип формирования паролей, шифров, сигнатур;
113) Назначение и основные принципы построения аппаратуры защиты;
114) Классификация средств активной защиты и характеристика их основных составляющих;
115) Определение и характеристика основных внутренних средств активной защиты;
116) Определение и характеристика основных внешних средств активной защиты;
117) Классификация средств пассивной защиты и характеристика их основных составляющих;
118) Назначение и основные принципы организации идентификации программ;
119) Назначение и основные принципы построения устройств контроля;
120) Общий состав требований по обеспечению ИБ;
121) Требования к программно аппаратным средствам;
122) Требования к подсистеме идентификации и аутентификации;
123) Требования к подсистеме управления доступом;
124) Требования к подсистеме протоколирования аудита;
125) Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
126) Требования к средствам обеспечения целостности;
127) Требования к средствам управления ИБ;
128) Общий состав требований к межсетевому экрану;
129) Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;
130) Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
131) Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
132) Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;
133) Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика.

Задания для опроса
по дисциплине Защита информационных процессов и систем

Вариант 1
№
Вопросы для текущего контроля и подготовки к экзамену
Модуль 1.

Вариант 2
Сущность и понятие информационной безопасности (ИБ);
Характеристика основных составляющих ИБ;
Значение ИБ для субъектов информационных отношений;

Вариант 3
Место ИБ в системе национальной безопасности;
Основные принципы обеспечения ИБ;
Классификация угроз ИБ;

Вариант 4
Состав и краткая характеристика внутренних и внешних источников угроз ИБ;
Состав и краткая характеристика основных угроз доступности;
Состав и краткая характеристика основных угроз целостности;

Вариант 5
Состав и краткая характеристика основных угроз конфиденциальности;
Модуль 2.
Классификация категорий хакеров и их целей;

Вариант 6
Состав и краткая характеристика организационно коммуникативных средств НСД;
Состав и краткая характеристика технических средств НСД;
Состав и краткая характеристика программных средств НСД;

Вариант 7
Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;
Классификация сетевых атак;
Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;

Вариант 8
Определение IP спуфинга и характеристика основных средств защиты от него;
Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;
Определение парольных атак и характеристика основных средств защиты от них;

Вариант 9
Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;
Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;
Модуль 3.

Вариант 10
Основные методы и условия неавторизованного доступа к ЛВС;
Краткая характеристика основных условий НСД к ЛВС;
Краткая характеристика основных условий раскрытия данных ЛВС;

Вариант 11

Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;

Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;

Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;

Вариант 12

Основные сервисы безопасности;

Основные принципы архитектурной безопасности и их краткая характеристика;

Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;

Вариант 13

Основные функции централизованного управления рисками и администрирования системы безопасности;

Основные функции защиты управления приложениями;

Основные функции защиты системы сетей;

Вариант 14

Основные функции защиты конечных пользователей;

Модуль 4.

Классификация средств защиты программного обеспечения и характеристика их основных категорий;

Вариант 15

Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;

Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;

Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";

Вариант 16

Классификация средства защиты с запросом информации и характеристика их основных составляющих;

Назначение и принцип формирования паролей, шифров, сигнатур;

Назначение и основные принципы построения аппаратуры защиты;

Вариант 17

Классификация средств активной защиты и характеристика их основных составляющих;

Определение и характеристика основных внутренних средств активной защиты;

Определение и характеристика основных внешних средств активной защиты;

Вариант 18

Классификация средств пассивной защиты и характеристика их основных составляющих;

Назначение и основные принципы организации идентификации программ;

Назначение и основные принципы построения устройств контроля;

Вариант 19

Модуль 5.

Общий состав требований по обеспечению ИБ;

Требования к программно аппаратным средствам;

Вариант 20

Требования к подсистеме идентификации и аутентификации;

Требования к подсистеме управления доступом;

Требования к подсистеме протоколирования аудита;

Вариант 21

Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;

Требования к средствам обеспечения целостности;

Требования к средствам управления ИБ;

Вариант 22

Общий состав требований к межсетевому экрану;

Модуль 6.

Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;

Вариант 23

Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;

Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;

Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;

Вариант 24

Показатели защищенности информации от НСД для компьютерных систем и их краткая характеристика. Показатели защищенности межсетевых экранов и их краткая характеристика.

Вопросы для подготовки к экзамену.

Сущность и понятие информационной безопасности (ИБ);

Вариант 25

Характеристика основных составляющих ИБ;

Значение ИБ для субъектов информационных отношений;

Место ИБ в системе национальной безопасности;

Вариант 26

Основные принципы обеспечения ИБ;

Классификация угроз ИБ;

Состав и краткая характеристика внутренних и внешних источников угроз ИБ;

Вариант 27

Состав и краткая характеристика основных угроз доступности;

Состав и краткая характеристика основных угроз целостности;

Состав и краткая характеристика основных угроз конфиденциальности;

Вариант 28

Классификация категорий хакеров и их целей;

Состав и краткая характеристика организационно коммуникативных средств НСД;

Состав и краткая характеристика технических средств НСД;

Вариант 29

Состав и краткая характеристика программных средств НСД;

Характеристика основных угроз ИБ при взаимодействии с Internet; требования к подсистеме защиты от угроз ИБ при взаимодействии с Internet;

Классификация сетевых атак;

Вариант 30

Определение сниффера пакетов и характеристика основных средств защиты от сниффинга;

Определение IP спуфинга и характеристика основных средств защиты от него;

Определение атак типа DoS ("отказ в обслуживании") и характеристика основных средств защиты от них;

Вариант 31

Определение парольных атак и характеристика основных средств защиты от них;

Определение атак на уровне приложений и типа Man in the Middle и характеристика основных средств защиты от них;

Определение сетевой разведки и переадресации портов и характеристика основных средств защиты от них;

Вариант 32

Основные методы и условия неавторизованного доступа к ЛВС;

Краткая характеристика основных условий НСД к ЛВС;

Краткая характеристика основных условий раскрытия данных ЛВС;

Вариант 33

Краткая характеристика неавторизованной модификации данных и программ и основных условий ее возникновения;

Краткая характеристика основных условий раскрытия и подмены трафика ЛВС;

Основные угрозы ИБ ЛВС при распределенном хранении файлов и удаленных вычислениях;

Вариант 34

Основные сервисы безопасности;

Основные принципы архитектурной безопасности и их краткая характеристика;

Структурная схема системы ЗИ для типовой информационной системы и краткая характеристика ее основных блоков;

Вариант 35

Основные функции централизованного управления рисками и администрирования системы безопасности;

Основные функции защиты управления приложениями;

Основные функции защиты системы сетей;

Вариант 36

Основные функции защиты конечных пользователей;

Классификация средств защиты программного обеспечения и характеристика их основных категорий;

Классификация средств защиты в составе вычислительной системы (ВС) и характеристика их основных составляющих;

Вариант 37

Принципы организации и технического исполнения защиты магнитных дисков и защитных механизмов устройств ВС;

Принципы организации и технического исполнения замков защиты и защиты типа "изменение функций";

Классификация средства защиты с запросом информации и характеристика их основных составляющих;

Вариант 38

Назначение и принцип формирования паролей, шифров, сигнатур;

Назначение и основные принципы построения аппаратуры защиты;

Классификация средств активной защиты и характеристика их основных составляющих;

Вариант 39

Определение и характеристика основных внутренних средств активной защиты;

Определение и характеристика основных внешних средств активной защиты;

Классификация средств пассивной защиты и характеристика их основных составляющих;

Вариант 40
Назначение и основные принципы организации идентификации программ;
Назначение и основные принципы построения устройств контроля;
Общий состав требований по обеспечению ИБ;

Вариант 41
Требования к программно аппаратным средствам;
Требования к подсистеме идентификации и аутентификации;
Требования к подсистеме управления доступом;

Вариант 42
Требования к подсистеме протоколирования аудита;
Требования к подсистеме защиты повторного использования объектов и к защите критичной информации;
Требования к средствам обеспечения целостности;

Вариант 43
Требования к средствам управления ИБ;
Общий состав требований к межсетевому экрану;
Подсистема управления доступом в автоматизированной системе и основные требования к ней для защиты от НСД;

Вариант 44
Подсистема регистрации и учета в автоматизированной системе и основные требования к ней для защиты от НСД;
Криптографическая подсистема ЗИ в автоматизированной системе и основные требования к ней для защиты от НСД;
Подсистема обеспечения целостности в автоматизированной системе и основные требования к ней для защиты от НСД;

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационные технологии и защита информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине Защита информационных процессов и систем

1) №
2) Принципы организации и технического исполнения замков защиты и защиты

типа “изменение функций”;
3) Определение IP спуфинга и характеристика основных средств защиты от него;

Составитель _____ Соколов С.В.

Заведующий кафедрой ИТ и ЗИ_____ Тищенко Е.Н.

«____» _____ 20____ г.

Критерии оценивания:

- 84-100 баллов (оценка «отлично») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов (оценка «хорошо») – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 баллов (оценка удовлетворительно) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- 0-49 баллов (оценка неудовлетворительно) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Лабораторные работы
по дисциплине Защита информационных процессов и систем

Лабораторная работа №1
(пусто)

Лабораторная работа №2
(пусто)

Лабораторная работа №3
(пусто)

Лабораторная работа №4
(пусто)

Лабораторная работа №5
(пусто)

Лабораторная работа №6
(пусто)

Лабораторная работа №7
(пусто)

Лабораторная работа №8
(пусто)

Лабораторная работа №9
(пусто)

2. Методические рекомендации по выполнению лабораторных работ

Лабораторные работы выполняются с учетом приобретенных знаний по предшествующим дисциплинам, теоретического материала дисциплины, с помощью и консультациями (при необходимости) преподавателя на занятиях.

3. Критерии оценки:

- 84-100 баллов (оценка «отлично») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов (оценка «хорошо») – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;
- 50-66 баллов (оценка удовлетворительно) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;
- 0-49 баллов (оценка неудовлетворительно) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

4. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена.

Экзамен проводится по расписанию экзаменационной сессии в устном виде. Количество вопросов в экзаменационном задании – 3. Объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры Информационные технологии и
защита информации
Протокол № 12 от 28.03.2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Защита информационных процессов и систем

Направление подготовки

10.03.01 Информационная безопасность

Профиль

10.03.01.02 Организация и технология защиты информации

Уровень образования

Бакалавриат

Составитель _____ Соколов С.В. профессор д.т.н. профессор
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Защита информационных процессов и систем» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки 10.03.01 «Информационная безопасность предусмотрены следующие виды занятий:

лекционные

лабораторные

В ходе лекционных занятий рассматриваются основные теоретические вопросы, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме;

– письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

По согласованию с преподавателем студент может подготовить реферат, доклад или сообщение по теме занятия. В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на аудиторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или контрольной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящим лабораторным занятиям по всем, обозначенным в рабочей программе дисциплины вопросам.

При реализации различных видов учебной работы используются разнообразные (в т.ч. интерактивные) методы обучения, в частности:

- интерактивная доска для подготовки и проведения лекционных занятий;

- размещение материалов курса в системе дистанционного обучения http://do.rsue.ru.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗа http://library.rsue.ru/. Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.