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

# МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
## Программно-аппаратные средства защиты информации

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) | | 7 (4.1) | | Итого | |
|---|---|---|---|---|---|---|
| Недель | 17,3 | | 17,3 | | | |
| Вид занятий | УП | РПД | УП | РПД | УП | РПД |
| Лекции | 18 | 18 | 36 | 36 | 54 | 54 |
| Лабораторные | 36 | 36 | 36 | 36 | 72 | 72 |
| В том числе инт. | | | 28 | 28 | 28 | 28 |
| Итого ауд. | 54 | 54 | 72 | 72 | 126 | 126 |
| Контактная работа | 54 | 54 | 72 | 72 | 126 | 126 |
| Сам. работа | 18 | 18 | 72 | 72 | 90 | 90 |
| Часы на контроль | | | 36 | 36 | 36 | 36 |
| Итого | 72 | 72 | 180 | 180 | 252 | 252 |

## 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): к.э.н., доцент, Радченко Ю.В. _____ 11.05.18

Зав. кафедрой: Тищенко Е.Н. _____ 11.05.18

Методическим советом направления: к.ф.-м.н., Декан, Карасев Д.Н. _____ 15.05.18

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): к.э.н., доцент, Радченко Ю.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): к.э.н., доцент, Радченко Ю.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): к.э.н., доцент, Радченко Ю.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): к.э.н., доцент, Радченко Ю.В. _____

| 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ | |
|---|---|
| 1.1 | ознакомление обучающихся с основными принципами использования программно-аппаратных комплексов защиты информации. |
| 1.2 | Задачи: |
| 1.3 | - сравнивать технико-эксплуатационные возможности устройств и систем защиты информации; |
| 1.4 | - расшифровывать и анализировать информацию о параметрах и характеристиках устройств с использованием различных источников; |
| 1.5 | - проектировать, планировать и разворачивать элементы комплексной системы защиты информации; |
| 1.6 | - устанавливать, настраивать, использовать программно-аппаратные средства защиты информации. |

| 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ | |
|---|---|
| Цикл (раздел) ООП: | Б1.Б.16 |
| **2.1** | **Требования к предварительной подготовке обучающегося:** |
| 2.1.1 | Необходимыми условиями для успешного освоения дисциплины являются знания, умения и навыки, полученные в результате изучения дисциплин: |
| 2.1.2 | Информатика |
| 2.1.3 | Аппаратные средства вычислительной техники |
| 2.1.4 | Основы информационной безопасности |
| 2.1.5 | Физико-технические основы обеспечения информационной безопасности |
| 2.1.6 | Проектно-технологическая практика |
| 2.1.7 | Методы атакующего воздействия на информационные ресурсы |
| 2.1.8 | Защита и обработка конфиденциальных документов |
| 2.1.9 | Физические основы защиты информации |
| 2.1.10 | Технологии и методы программирования |
| **2.2** | **Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** |
| 2.2.1 | Комплексное обеспечение защиты информации объекта информатизации |
| 2.2.2 | Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты |
| 2.2.3 | Методология и организация информационно-аналитической деятельности |
| 2.2.4 | Подготовка к сдаче и сдача государственного экзамена |
| 2.2.5 | Преддипломная практика |
| 2.2.6 | Технология сбора и анализа информации |

| 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ |
|---|
| **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 оценки защищенности информационных ресурсов, определения угроз и способов их реализации |
| **Уметь:** |
| пользоваться способностью к анализу структуры и содержания информационных процессов функционирования объекта защиты |
| **Владеть:** |
| навыками анализа и использования формальных методов оценки объектов защиты |
| **ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации** |
| **Знать:** |
| современные программно-аппаратные, программные и технические средства защиты информации |
| **Уметь:** |
| сравнивать технико-эксплуатационные возможности устройств и систем защиты информации |
| **Владеть:** |
| навыками установки, настройки и обслуживания программных, программно-аппаратных и технических средств защиты информации в профессиональной деятельности |
| **ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач** |

| |
|---|
| **Знать:** |
| общие характеристики процессов сбора, передачи, обработки и накопления информации, технических средств реализации информационных процессов |
| **Уметь:** |
| расшифровывать и анализировать информацию о параметрах и характеристиках устройств с использованием различных источников |
| **Владеть:** |
| навыками использования программных средств различного назначения для решения профессиональных задач |
| **ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты** |
| **Знать:** |
| принципы построения и организации функционирования современных устройств и систем хранения, обработки, поиска и передачи информации, технико-эксплуатационные показатели средств преобразования информации, используемых при обработке экономической информации |
| **Уметь:** |
| проектировать, планировать и разворачивать элементы комплексной системы защиты информации |
| **Владеть:** |
| навыками планирования и организации работ по реализации политики информационной безопасности |
| **ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации** |
| **Знать:** |
| методы и подходы к проведению эксперементальных исследований системы защиты информации |
| **Уметь:** |
| устанавливать, настраивать, использовать программно-аппаратные средства защиты информации |
| **Владеть:** |
| навыками использования программно-аппаратных средств защиты информации, планирования и проведения экспериментальных исследований |

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

| Код занятия | Наименование разделов и тем /вид занятия/ | Семестр / Курс | Часов | Компетен-ции | Литература | Интер акт. | Примечание |
|---|---|---|---|---|---|---|---|
| | **Раздел 1. Основные понятия программно-аппаратной защиты информации. Управление доступом к компонентам информационных систем** | | | | | | |
| 1.1 | Тема 1.1 "Основные понятия программно-аппаратной защиты информации" Предмет и задачи программно-аппаратной защиты информации. Основные понятия. Уязвимость информационных систем. Политика безопасности в информационных системах. Оценка защищенности. Механизмы защиты. /Лек/ | 6 | 2 | ОПК-7 ПК-1 ПК-2 ПК-4 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 0 | |
| 1.2 | Тема 1.2 "Идентификация пользователей информационных систем -субъектов доступа к данным" Идентификация и аутентификация пользователей. Взаимная проверка подлинности. Протоколы идентификации. /Лек/ | 6 | 4 | ОПК-7 ПК-1 ПК-2 ПК-4 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.3 | Тема 1.3 "Средства и методы ограничения доступа к ресурсам информационных систем"<br>Защита информации от несанкционированного доступа. Система разграничения доступа к информации в компьютерных системах. Методы и средства ограничения доступа к компонентам ЭВМ. /Лек/ | 6 | 4 | ОПК-7 ПК-1 ПК-2 ПК-4 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |
| 1.4 | Тема 1.5 "Применение средств защиты информации от несанкционированного доступа для организации защищенных компьютерных систем"<br>Методы противодействия несанкционированному доступу. Программно-аппаратные комплексы защиты информации от несанкционированного доступа /Лек/ | 6 | 4 | ОПК-7 ПК-1 ПК-2 ПК-4 | Л1.1 Л1.3 Л2.1 Л3.1 Э1 | 0 | |
| 1.5 | Тема 1.4 "Организация и контроль доступа к файлам"<br>Шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам. Способы фиксации факта доступа. Надежность систем ограничения доступа.<br>Защита файлов от изменения. /Лек/ | 6 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 0 | |
| 1.6 | Тема 1.2 "Идентификация пользователей информационных систем -субъектов доступа к данным"<br>Запуск менеджера виртуальных машин. Установка виртуальных машин: MS Windows Server, MS Windows 7. Настройка одноранговой сети. Создание учетных записей пользователей. Настройка локальных политик паролей. Создание иерархической структуры сети. Установка контроллера домена. Управление учетными записями пользователей. /Лаб/ | 6 | 8 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |
| 1.7 | Тема 1.3 "Средства и методы ограничения доступа к ресурсам информационных систем"<br>Ознакомление с аппаратными комплексами защиты от несанкционированного доступа к ИС. Программно-аппаратный комплекс "Соболь": ознакомление, установка, настройка. Аппаратные средства биометрической идентификации. /Лаб/ | 6 | 10 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 0 | |
| 1.8 | Тема 1.4 "Организация и контроль доступа к файлам"<br>Создание на виртуальном сервере сетевого ресурса. Настройка доступа к созданному ресурсу в одноранговой и иерархической сети. Виды доступа. Наследование прав на сетевые ресурсы. Использование групп безопасности для организации доступа к сетевым рессурсам. /Лаб/ | 6 | 8 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.9 | Тема 1.5 "Применение средств защиты информации от несанкционированного доступа для организации защищенных компьютерных систем" Установка, настройка, эксплуатация программно-аппаратных средств защиты информации от несанкционированного доступа /Лаб/ | 6 | 10 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 0 | |
| 1.10 | Удаленные сетевые атаки /Ср/ | 6 | 8 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |
| 1.11 | Основы межсетевого взаимодействия /Ср/ | 6 | 10 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |
| 1.12 | Зачет /Зачёт/ | 6 | 0 | ОПК-7 ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Л3.2 Э1 | 0 | |
| | **Раздел 2. Защита данных от стандартных угроз** | | | | | | |
| 2.1 | Тема 2.1 "Межсетевые экраны" Развитие технологий межсетевого экранирования. Классификации межсетевых экранов. Способы применения межсетевых экранов. Обход межсетевых экранов. Показатели защищенности межсетевых экранов. /Лек/ | 7 | 6 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 2 | |
| 2.2 | Тема 2.2 "Резервное копирование данных" Цели и задачи резервного процедуры резервного копирования данных. Планирование процедуры резервного копирования. Основные требования, предъявляемые к процедуре резервного копирования данных /Лек/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 2 | |
| 2.3 | Тема 2.3 "Защита данных от вредоносных программ" Компьютерные вирусы. Классификация компьютерных вирусов. Угрозы компьютерных вирусов. Защита данных от вредоносного программного обеспечения. Антивирусное программное обеспечение. /Лек/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 2 | |
| 2.4 | Тема 2.4 "Аппаратные средства повышения отказоустойчивости и надежности информационных систем" Понятия надежности и отказоустойчивости. Защита систем от проблем с электропитанием. Виды устройств защиты. Классификация источников бесперебойного питания, области применения. Дублирование - как основной способ повышения отказоустойчивости. Дублирование серверных центров и отдельных элементов информационной системы. RAID - массивы: виды, способы использования. Аппаратный и программный RAID. /Лек/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 1 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2.5 | Тема 2.1 "Межсетевые экраны" Установка в виртуальную сетевую среду на сервер межсетевого экрана. Первичная настройка межсетевого экрана. Формирование правил фильтрации пакетов. Проверка уровня защищенности требованиям. /Лаб/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 4 | |
| 2.6 | Тема 2.2 "Защита данных от вредоносных программ" Установка в виртуальной среде антивирусного комплекса. Настройка основных параметров. Сканирование дисков и объектов. /Лаб/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 3 | |
| 2.7 | Тема 2.3 "Аппаратные средства повышения отказоустойчивости и надежности информационных систем" Работа с программным RAID в Windows сервер. Создание дополнительного виртуального жесткого диска. Подключение диска к виртуальному серверу. Создание RAID-массива. Генерация события отказа и оценка работоспособности RAID- массива. /Лаб/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 3 | |
| | **Раздел 3. Организация защиты данных при сетевом взаимодействии** | | | | | | |
| 3.1 | Тема 3.1 "Основы межсетевого взаимодействия" Основы передачи данных в сетях. Инкапсуляция пакетов. Виды адресации в TCP\IP сетях. Основные протоколы передачи данных IP,TCP,UDP. /Лек/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 1 | |
| 3.2 | Тема 3.2 "Удаленные сетевые атаки" Обобщенный сценарий атак. Атаки типа "отказ в обслуживании". Атаки на сетевые протоколы. /Лек/ | 7 | 6 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 1 | |
| 3.3 | Тема 3.3 "Защищенные протоколы передачи данных" Защищенные протоколы передачи данных. Виртуальные частные сети (VPN). Протоколы VPN канального уровня. Протокол IPSEC. Режимы работы протокола. Протоколы аутентификации. Построение VPN /Лек/ | 7 | 4 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 1 | |
| 3.4 | Тема 3.4 "Системы обнаружения атак и вторжений" Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие способы обнаружения вторжений. системы предупреждения вторжений. /Лек/ | 7 | 4 | ОПК-7 ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л1.4 Л2.1 Л3.1 Э1 | 2 | |
| 3.5 | Тема 3.1 "Основы межсетевого взаимодействия" Установка и настройка утилиты "Сетевой монитор". Оценка сетевого трафика. Сбор трафика. Анализ трафика. Определение принадлежности пакета. Перехват передаваемых данных. /Лаб/ | 7 | 12 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 3 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3.6 | Тема 3.2 "Защищенные протоколы передачи данных"<br>Разворачивание архитектуры VPN с использованием стандартных средств защиты Windows сервер. /Лаб/ | 7 | 12 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 3 | |
| 3.7 | Защищенные протоколы передачи данных /Ср/ | 7 | 12 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 | 0 | |
| 3.8 | Вопросы для самостоятельной подготовки с учетом интересов обучающегося:<br>1) Типы и применение RAID массивов.<br>2) Аппаратные устройства для разграничения доступа в сети.<br>3) Выбор аппаратных компонентов для организации серверных центров.<br>4) Система безопасности Windows.<br>5) Политика безопасности, наследование политики безопасности<br>6) Протокол безопасности Kerberos.<br>7) Маршрутизация. Таблицы маршрутизации<br>8) Службы Windows для мониторинга и оптимизации.<br>9) Протокол безопасности IpSec /Ср/ | 7 | 50 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1 Э1 | 0 | |
| 3.9 | Курсовой проект. Перечень тем представлен в Приложении 1 к рабочей программе дисциплины. /Ср/ | 7 | 10 | ОПК-7 ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.4 Л2.1 Л3.1 Л3.2 Э1 | 0 | |
| 3.10 | ЭКЗАМЕН /Экзамен/ | 7 | 36 | ПК-1 ПК-2 ПК-4 ПК-12 | Л1.1 Л1.2 Л1.3 Л2.1 Л3.2 Э1 | 0 | |

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачету:
1) Операционные системы Windows
2) Выбор аппартной конфигурации сервера
3) Этапы установки Windows сервера
4) Выполнение основных настроек сервера
5) Идентификация субъекта персональных данных
6) Процесс идентификации и аутентификации пользователей
7) Защита информации от НСД.
8) Система разграничения доступа к информации в информационных системах
9) Политики безопасности
10) Локлаьная и глобальная политика безопасности домена
11) Протоколы идентификации
12) Взаимная идентификация
13) Одноранговые сети
14) Иерархические сети
15) Принципиальные различия одноранговых и иерархических сетей
16) Службы каталогов
17) Служба Active Directory
18) Группы безопасности
19) Распределение доступа с использованием групп безопасности
20) Управление учетными записями пользователей

Вопросы к экзамену:
1) Семейство ОС Windows.
2) Этапы установки Windows.
3) Аппаратные требования Windows.
4) RAID. Аппаратный и программный. Типы.
5) RAID в Windows.
6) Работа с дисками в Windows.
7) Источники резервного питания
8) Резервное копирование данных.
9) Аппаратные устройства для разграничения доступа в сети.
10) Служба каталогов Windows.
11) Домен, дерево, лес в службе каталогов Windows.
12) Выбор аппаратных компонентов для организации серверных центров.
13) Служба каталогов Active Directory.
14) Установка и настройка AD.
15) Управление пользователями с помощью AD.
16) Группы в AD. Типы групп.
17) Разграничение доступа к ресурсам.
18) Система безопасности Windows.
19) Политика безопасности, наследование политики безопасности
20) Протокол безопасности Kerberos.
21) Firewall: назначение, принцип работы.
22) Microsoft ISA Server: особенности установки и настройки.
23) Виды адресаций в TCP/IP сетях
24) IP адрес: назначение, структура, применение
25) DNS имя: назначение, структура, применение
26) Семиуровневая модель OSI.
27) Характеристика стэка протоколов TCP/IP.
28) Виды адресации в IP сетях.
29) Протокол IP: назначение, структура заголовка, принципы работы
30) Протокол TCP: назначение, структура заголовка, основные режимы работы
31) Маршрутизация. Таблицы маршрутизации
32) Службы Windows для мониторинга и оптимизации.
33) Мониторинг и оптимизация производительности дисков.
34) Работа с дисковыми квотами.
35) Сжатие и шифрование данных средствами ОС.
36) Консоль "Производительность": назначение, состав.
37) Оснастка "Системный монитор"
38) Оснастка "Журналы"
39) Утилита "Диспетчер задач": назначение, функции.
40) Описание протоколов VPN
41) Компоненты VipNet
42) Secret Net назначение и функции
43) Основные особенности использования Secret Net
44) Сравнительная характеристика Proxy и Nat серверов
45) Протокол безопасности IpSec
46) Программно-аппаратный комплекс "Соболь": назначение, установка, настройка

**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 |
|---|---|---|---|---|
| Л1.1 | Хорев П. Б. | Методы и средства защиты информации в компьютерных системах: учеб. пособие | М.: Академия, 2005 | 20 |
| Л1.2 | Иртегов Д. В. | Введение в сетевые технологии | СПб.: БХВ-Петербург, 2004 | 30 |
| Л1.3 | | Компьютерные системы и сети: Учеб. пособие | М.: Финансы и статистика, 1999 | 55 |

| | Авторы, составители | Заглавие | Издательство, год | Колич-во |
|---|---|---|---|---|
| Л1.4 | Сычев Ю. Н. | Основы информационной безопасности: учебно-практическое пособие | Москва: Евразийский открытый институт, 2010 | http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей |
| **6.1.2. Дополнительная литература** | | | | |
| | Авторы, составители | Заглавие | Издательство, год | Колич-во |
| Л2.1 | Соколов С. В., Серпенинов О. В., Тищенко Е. Н. | Криптографическая защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность" | Ростов н/Д: Изд-во РГЭУ "РИНХ", 2011 | 66 |
| Л2.2 | Титов А. А. | Инженерно-техническая защита информации: учебное пособие | Томск: Томский государственный университет систем управления и радиоэлектроники, 2010 | http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей |
| **6.1.3. Методические разработки** | | | | |
| | Авторы, составители | Заглавие | Издательство, год | Колич-во |
| Л3.1 | Шаньгин В. Ф. | Комплексная защита информации в корпоративных системах: учеб. пособие для студентов вузов, обучающихся по напр. 230100 "Информатика и вычислит. техника" | М.: ФОРУМ, 2010 | 30 |
| Л3.2 | Тищенко Е. Н., Щербаков С. М., Денисов М. Ю., Хубаев Г. Н. | Экономические информационные системы и их безопасность: разработка, применение и сопровождение: материалы регион. науч.-практ. конф. профессор.-преподават. состава, молодых ученых, аспирантов и студентов, п. Архыз 1-5 окт. 2009 г. | Ростов н/Д: Изд-во РГЭУ (РИНХ), 2010 | 5 |
| **6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"** | | | | |
| Э1 | ФСТЭК России/fstec.ru | | | |
| **6.3. Перечень программного обеспечения** | | | | |
| 6.3.1 | Microsoft Office | | | |
| 6.3.2 | MS Windosw | | | |
| 6.3.3 | | | | |
| 6.3.4 | MS Windows Server | | | |
| 6.3.5 | Oracle VM Virtual Box | | | |
| **6.4 Перечень информационных справочных систем** | | | | |
| 6.4.1 | Консультант плюс | | | |
| 6.4.2 | 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 освоению 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 № 10 от 10.03.2018 г.
Зав.кафедрой _____ Тищенко Е.Н.

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Программно-аппаратные средства защиты информации

Направление подготовки
10.03.01 Информационная безопасность

Профиль
10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Радченко Ю.В. доцент к.э.н. доцент
(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

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 |
|---|---|---|---|
| ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | | | |
| З. - современные достижения науки и техники в области защиты информации; | Семейство ОС Windows. Этапы установки Windows. Аппаратные требования Windows. | полнота и содержательность ответа умение приводить примеры | О |
| У. - сравнивать технико-эксплуатационные возможности устройств и систем защиты информации; | RAID. Аппаратный и программный. Типы. RAID в Windows. Работа с дисками в Windows. | полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач | О, ЛР, КП |
| В. использования программно-аппаратных средств защиты информации в профессиональной деятельности | Источники резервного питания Резервное копирование данных. Аппаратные устройства для разграничения доступа в сети. | полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач | О, ЛР, КП |
| ПК-2 способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач | | | |
| З. - общие характеристики процессов сбора, передачи, обработки и накопления информации, технических средств реализации информационных процессов; | Служба каталогов Windows. Домен, дерево, лес в службе каталогов Windows. Выбор аппаратных компонентов для организации серверных центров. | полнота и содержательность ответа умение приводить примеры | О |
| У. - расшифровывать и анализировать информацию о параметрах и характеристиках устройств с использованием различных источников; | Служба каталогов Active Directory. Установка и настройка AD. Управление пользователями с помощью AD. | полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач | О, ЛР, КП |
| В. использования | Группы в AD. Типы групп. | полнота и | О, ЛР, КП |

| | | | |
|---|---|---|---|
| программно-аппаратных средств защиты информации в профессиональной деятельности | Разграничение доступа к ресурсам.<br>Система безопасности Windows. | содержательность ответа<br>умение приводить примеры<br>умение самостоятельно находить решение поставленных задач | |
| ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты | | | |
| З. - принципы построения и организации функционирования современных устройств и систем хранения, обработки, поиска и передачи информации;<br>- технико-эксплуатационные показатели средств преобразования информации, используемых при обработке экономической информации; | Политика безопасности, наследование политики безопасности<br>Протокол безопасности Kerberos.<br>Firewall: назначение, принцип работы. | полнота и содержательность ответа<br>умение приводить примеры | О |
| У. - проектировать, планировать и разворачивать элементы комплексной системы защиты информации; | Microsoft ISA Server: особенности установки и настройки.<br>Виды адресаций в TCP/IP сетях<br>IP адрес: назначение, структура, применение | полнота и содержательность ответа<br>умение приводить примеры<br>умение самостоятельно находить решение поставленных задач | О, ЛР, КП |
| В. использования программно-аппаратных средств защиты информации в профессиональной деятельности | DNS имя: назначение, структура, применение<br>Семиуровневая модель OSI.<br>Характеристика стэка протоколов TCP/IP. | полнота и содержательность ответа<br>умение приводить примеры<br>умение самостоятельно находить решение поставленных задач | О, ЛР, КП |
| ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации | | | |
| З. - технико-эксплуатационные показатели программно-аппаратных средств защиты информации. | Виды адресации в IP сетях.<br>Протокол IP: назначение, структура заголовка, принципы работы<br>Протокол TCP: назначение, структура заголовка, основные режимы работы | полнота и содержательность ответа<br>умение приводить примеры | О |
| У. - устанавливать, настраивать, использовать программно-аппаратные средства защиты информации. | Маршрутизация. Таблицы маршрутизации<br>Службы Windows для мониторинга и оптимизации.<br>Мониторинг и оптимизация производительности дисков. | полнота и содержательность ответа<br>умение приводить примеры<br>умение самостоятельно находить решение поставленных задач | О, ЛР, КП |
| В. использования программно-аппаратных | Работа с дисковыми квотами. | полнота и содержательность ответа | О, ЛР, КП |

| | | | |
|---|---|---|---|
| средств защиты информации в профессиональной деятельности | Сжатие и шифрование данных средствами ОС. Консоль "Производительность": назначение, состав. | умение приводить примеры умение самостоятельно находить решение поставленных задач | |

О – опрос, ЛР- лабораторная работа, КП – курсовой проект

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, тематика курсовых проектов, экзаменационный билет.

### Вопросы к экзамену
### по дисциплине Программно-аппаратные средства защиты информации

1) Семейство ОС Windows.
2) Этапы установки Windows.
3) Аппаратные требования Windows.
4) RAID. Аппаратный и программный. Типы.
5) RAID в Windows.
6) Работа с дисками в Windows.
7) Источники резервного питания
8) Резервное копирование данных.
9) Аппаратные устройства для разграничения доступа в сети.
10) Служба каталогов Windows.
11) Домен, дерево, лес в службе каталогов Windows.
12) Выбор аппаратных компонентов для организации серверных центров.
13) Служба каталогов Active Directory.
14) Установка и настройка AD.
15) Управление пользователями с помощью AD.
16) Группы в AD. Типы групп.
17) Разграничение доступа к ресурсам.
18) Система безопасности Windows.
19) Политика безопасности, наследование политики безопасности

20) Протокол безопасности Kerberos.
21) Firewall: назначение, принцип работы.
22) Microsoft ISA Server: особенности установки и настройки.
23) Виды адресаций в TCP/IP сетях
24) IP адрес: назначение, структура, применение
25) DNS имя: назначение, структура, применение
26) Семиуровневая модель OSI.
27) Характеристика стэка протоколов TCP/IP.
28) Виды адресации в IP сетях.
29) Протокол IP: назначение, структура заголовка, принципы работы
30) Протокол TCP: назначение, структура заголовка, основные режимы работы
31) Маршрутизация. Таблицы маршрутизации
32) Службы Windows для мониторинга и оптимизации.
33) Мониторинг и оптимизация производительности дисков.
34) Работа с дисковыми квотами.
35) Сжатие и шифрование данных средствами ОС.
36) Консоль "Производительность": назначение, состав.
37) Оснастка "Системный монитор"
38) Оснастка "Журналы"
39) Утилита "Диспетчер задач": назначение, функции.
40) Описание протоколов VPN
41) Компоненты VipNet
42) Secret Net назначение и функции
43) Основные особенности использования Secret Net
44) Сравнительная характеристика Proxy и Nat серверов
45) Протокол безопасности IpSec
46) Программно-аппаратный комплекс "Соболь": назначение, установка, настройка

## Задания для опроса
## по дисциплине Программно-аппаратные средства защиты информации

Вариант 1
Семейство ОС Windows.
Этапы установки Windows.
Аппаратные требования Windows.

Вариант 2
RAID. Аппаратный и программный. Типы.
RAID в Windows.
Работа с дисками в Windows.

Вариант 3
Источники резервного питания
Резервное копирование данных.
Аппаратные устройства для разграничения доступа в сети.

Вариант 4
Служба каталогов Windows.
Домен, дерево, лес в службе каталогов Windows.
Выбор аппаратных компонентов для организации серверных центров.

Вариант 5
Служба каталогов Active Directory.

Установка  и настройка AD.
Управление пользователями с помощью AD.

Вариант 6
Группы в AD. Типы групп.
Разграничение доступа к ресурсам.
Система безопасности Windows.

Вариант 7
Политика безопасности, наследование политики безопасности
Протокол безопасности Kerberos.
Firewall: назначение, принцип работы.

Вариант 8
Microsoft ISA Server: особенности установки и настройки.
Виды адресаций в TCP/IP сетях
IP адрес: назначение, структура, применение

Вариант 9
DNS имя: назначение, структура, применение
Семиуровневая модель OSI.
Характеристика стэка протоколов TCP/IP.

Вариант 10
Виды адресации в IP сетях.
Протокол IP: назначение, структура заголовка, принципы работы
Протокол TCP: назначение, структура заголовка, основные режимы работы

Вариант 11
Маршрутизация. Таблицы маршрутизации
Службы Windows для мониторинга и оптимизации.
Мониторинг и оптимизация производительности дисков.

Вариант 12
Работа с дисковыми квотами.
Сжатие и шифрование данных средствами ОС.
Консоль "Производительность": назначение, состав.

Вариант 13
Оснастка "Системный монитор"
Оснастка "Журналы"
Утилита "Диспетчер задач": назначение, функции.

Вариант 14
Описание протоколов VPN
Компоненты VipNet
Secret Net назначение и функции

Вариант 15
Основные особенности использования Secret Net
Сравнительная характеристика  Proxy  и Nat серверов
Протокол безопасности IpSec

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 Программно-аппаратные средства защиты информации**

1) Семейство ОС Windows.
2) Группы в AD. Типы групп.
3) Маршрутизация. Таблицы маршрутизации

Составитель _____ Радченко Ю.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.

**Темы курсовых проектов**
**по дисциплине Программно-аппаратные средства защиты информации**

В рамках курсового проекта необходимо проанализировать структуры предприятия, угрозы информационной безопасности для выбранного предприятия и выбрать наиболее актуальные, предложить комплекс административных и программно-аппаратных мер защиты данных.

**Вариант 1.**

Оптовая фирма по продаже продуктов питания в связи с расширением своей деятельности реорганизует свою структуру. Имеется бухгалтерия и отдел продаж. Планируется создание коммерческого отдела, для решения вопросов стратегического планирования. Существующие отделы снабжены компьютерами и несвязанными сегментами локальной сети.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.
2. Разработать перечень административных мероприятий по защите данных.
3. Осуществить выбор программных и аппаратных средств защиты данных.

**Вариант 2.**

Создается инвестиционная компания.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.
2. Разработать перечень административных мероприятий по защите данных.
3. Осуществить выбор программных и аппаратных средств защиты данных.

**Вариант 3.**

Крупная торговая фирма производит модернизацию инфраструктуры и существующей информационной системы. Фирма имеет локальную сеть, объединяющую все подразделения. Существует подключение к сети Internet. Основное внимание фирма уделяет развитию сети филиалов и в связи с этим необходимо организовать взаимодействие филиалов и головной компании.

Требуется:

1. Разработать структуру сети, объединяющей все филиалы, с учетом требований информационной безопасности. Разработать типовую схему локальной сети филиала.
2. Разработать перечень административных мероприятий по защите данных.
3. Осуществить выбор программных и аппаратных средств защиты данных.

**Вариант 4.**

Создается коммерческий банк.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.
2. Разработать перечень административных мероприятий по защите данных.
3. Осуществить выбор программных и аппаратных средств защиты данных.

**Вариант 5.**

Сеть розничных магазинов планирует организовать Internet-магазин и объединить локальные сети в одну общую сеть.

Требуется:

1. Разработать структуру сети, объединяющей все магазины, с учетом требований информационной безопасности.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных для сети и электронного магазина.

**Вариант 6.**

На производственном предприятии принято решение о внедрении информационных технологий и создании локальной сети.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных.

**Вариант 7.**

Университет модернизирует локальную сеть и внедряет дистанционное обучение.

Требуется:

1. Разработать структуру локальной сети, с учетом требований информационной безопасности. Предусмотреть выход в Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных для сети и отделения дистанционного образования.

**Вариант 8.**

Свободная тема. Требует утверждения у преподавателя.

**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.

**Лабораторные работы**
**по дисциплине Программно-аппаратные средства защиты информации**

Лабораторная работа №1

Запуск менеджера виртуальных машин. Установка виртуальных машин: MS Windows Server, MS Windows 7. Настройка одноранговой сети. Создание учетных записей пользователей. Настройка локальных политик паролей.

Создание иерархической структуры сети. Установка контроллера домена. Управление учетными записями пользователей.

Лабораторная работа №2

Ознакомление с аппаратными комплексами защиты от несанкционированного доступа к ИС. Программно-аппаратный комплекс «Соболь»: ознакомление, установка, настройка. Аппаратные средства биометрической идентификации.

Лабораторная работа №3

Создание на виртуальном сервере сетевого ресурса. Настройка доступа к созданному ресурсу в одноранговой и иерархической сети. Виды доступа. Наследование прав на сетевые ресурсы. Использование групп безопасности для организации доступа к сетевым рессурсам.

Лабораторная работа №4

Установка в виртуальную сетевую среду на сервер межсетевого экрана. Первичная настройка межсетевого экрана. Формирование правил фильтрации пакетов. Проверка уровня защищенности требованиям.

Лабораторная работа №5

Установка в виртуальной среде антивирусного комплекса. Настройка основных параметров. Сканирование дисков и объектов.

Лабораторная работа №6

Работа с программным RAID в Windows сервер. Создание дополнительного виртуального жесткого диска. Подключение диска к виртуальному серверу. Создание RAID–массива. Генерация события отказа и оценка работоспособности RAID-массива.

Лабораторная работа №7

Установка и настройка утилиты «Сетевой монитор». Оценка сетевого трафика. Сбор трафика. Анализ трафика. Определение принадлежности пакета. Перехват передаваемых данных.

Лабораторная работа №8

Разворачивание архитектуры VPN с использованием стандартных средств защиты Windows сервер.

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, защиты курсового проекта.

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.

Защита курсового проекта проводится за счет времени, отведенного на освоение дисциплины.

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 № 10 от 17.05.18 г.
Зав.кафедрой _____ Тищенко Е.Н.

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Направление подготовки

10.03.01 Информационная безопасность

Профиль

10.03.01.02 Организация и технология защиты информации

Уровень образования

Бакалавриат

Составитель _____ Радченко Ю.В. доцент к.э.н. доцент
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Программно-аппаратные средства защиты информации» 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.