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
Технология сбора и анализа 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>)	8 (4.2)		Итого	
Недель	7,8			
Вид занятий	УП	РПД	УП	РПД
Лекции	24	24	24	24
Лабораторные	32	32	32	32
В том числе инт.	10	10	10	10
Итого ауд.	56	56	56	56
Контактная работа	56	56	56	56
Сам. работа	52	52	52	52
Итого	108	108	108	108

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.т.н., доцент, Серпенинов Олег Витальевич _____ 11.05.18

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____ 11.05.18

Методическим советом направления: к.ф.м.н., декан, Карасев Денис Николаевич _____ 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 д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

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 д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

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: д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

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: д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью дисциплины является ознакомление студентов с основными технологиями сбора и анализа информации.
1.2	Задачи дисциплины:дать представление об основных типах технических и программных средств, используемых для сбора и анализа информации, их технико-экономических характеристиках, принципах построения и функционирования;приобретение теоретических знаний и навыков в сравнительной оценке современных устройств, перспективах развития; получить навыки по использованию современного инструментария предназначенного для построения современных систем защиты информации.

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 дисциплины являются навыки, знания и умения, поученые в результате изучения дисциплин:
2.1.2	Системы защищенного электронного документооборота
2.1.3	Теория информационной безопасности и методология защиты информации
2.1.4	Защита и обработка конфиденциальных документов
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Преддипломная практика
2.2.2	Подготовка к сдаче государственного экзамена

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
Знать:
три сандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Уметь:
выполнять техническое обслуживание вычислительной техники
Владеть:
объяснить решённые на аудиторных занятиях задачи и задания с изменёнными исходными данными
ПК-8: способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
Знать:
Принципы построения и организацию функционирования современных компьютеров и вычислительных сетей. Структуру внешней среды компьютера.
Уметь:
Выполнять выбор локальной сети и способа подключения к INTERNET.
Владеть:
информацией о перспективах развития вычислительных систем и сетей, о средствах подключения к INTERNET.
ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
Знать:
Принципы построения и организацию функционирования современных компьютеров и вычислительных сетей. Структуру внешней среды компьютера.
Уметь:
Выполнять выбор локальной сети и способа подключения к INTERNET.
Владеть:
информацией о перспективах развития вычислительных систем и сетей, о средствах подключения к INTERNET.

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. Аппаратные средства сбора информации						

1.1	"Задачи сбора и анализа информации"; Основные определения и понятия. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
1.2	"Аппаратные средства сбора информации с использованием технических каналов информации":технические и программные средства, используемые для сбора и анализа информации, их технико-экономические характеристики. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
1.3	"Аппаратные средства сбора информации с использованием технических каналов информации":технические и программные средства, используемые для сбора и анализа информации, их технико-экономические характеристики. /Ср/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
1.4	Планирование процедуры сбора информации. /Лаб/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
1.5	Планирование процедуры сбора информации. /Ср/	8	4	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
1.6	Работа с техническими средствами обнаружения закладок. /Лаб/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
1.7	Работа с техническими средствами обнаружения закладок. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 2. Защита данных от НСД						
2.1	"Основные подходы к защите данных от НСД":классификация и характеристика основных подходов к защите данных от НСД;способы фиксации факта доступа. /Лек/	8	2	ПК-7 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.2	"Основные подходы к защите данных от НСД":классификация и характеристика основных подходов к защите данных от НСД;способы фиксации факта доступа. /Ср/	8	2	ПК-7 ПК-8	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.3	"Защита сетевого файлового ресурса":способы фиксации факта доступа к файлам. /Лек/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
2.4	"Защита сетевого файлового ресурса":способы фиксации факта доступа к файлам. /Ср/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.5	"Надежность систем ограничения доступа":основные направления повышения надежности систем ограничения доступа;сегментирование локальных сетей. /Лек/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
2.6	"Надежность систем ограничения доступа":основные направления повышения надежности систем ограничения доступа;сегментирование локальных сетей. /Лаб/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	

2.7	"Использование коммутаторов для организации виртуальных подсетей": стандартные способы разграничения доступа. /Лек/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
2.8	"Использование коммутаторов для организации виртуальных подсетей": стандартные способы разграничения доступа. /Ср/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.9	Организация защиты данных от НСД. Фиксация доступа к файлам и другим элементам ИС. /Лаб/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.10	Организация защиты данных от НСД. Фиксация доступа к файлам и другим элементам ИС. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.11	Установка ПО VIP NET. /Лаб/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.12	Установка ПО VIP NET. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.13	Настройка ПО VIP NET. Организация защищенного туннеля. Контроль процесса передачи данных. /Лаб/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.14	Настройка ПО VIP NET. Организация защищенного туннеля. Контроль процесса передачи данных. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.15	Настройка ПО VIP NET.Решение проблем взаимодействия систем в процессе передачи. /Лаб/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
2.16	Настройка ПО VIP NET.Решение проблем взаимодействия систем в процессе передачи. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 3. Программно-аппаратные комплексы организации защищенного информационного обмена						
3.1	"Электронная подпись";особенности использования электронной подписи; программно-аппаратные способы шифрования. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
3.2	"Электронная подпись";особенности использования электронной подписи; программно-аппаратные способы шифрования. /Ср/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.3	"Построение аппаратных компонент криптозащиты данных":защита алгоритма шифрования. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
3.4	"Методы и средства ограничения доступа к компонентам ЭВМ": характеристика основных методов и средств ограничения доступа к компонентам ЭВМ. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	

3.5	"Организация мероприятий по контролю сетевого трафика":основные организационные мероприятия по контролю сетевого трафика и их характеристика. /Лек/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
3.6	"Организация мероприятий по контролю сетевого трафика":основные организационные мероприятия по контролю сетевого трафика и их характеристика. /Ср/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.7	Организация защиты данных от НСД. Фиксация доступа к файлам и другим элементам ИС. /Лаб/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.8	Организация защиты данных от НСД. Фиксация доступа к файлам и другим элементам ИС. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.9	Установка и настройка аппаратной части ПАК «Соболь». /Лаб/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.10	Установка и настройка аппаратной части ПАК «Соболь». /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.11	Организация мероприятий по контролю сетевого трафика Использование специального программного обеспечения. /Лаб/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
3.12	Организация мероприятий по контролю сетевого трафика Использование специального программного обеспечения. /Ср/	8	4	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
	Раздел 4. Защита от разрушающих программных воздействий						
4.1	"Компьютерные вирусы как особый класс разрушающих программных воздействий":классификация и характеристика компьютерных вирусов. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
4.2	"Компьютерные вирусы как особый класс разрушающих программных воздействий":классификация и характеристика компьютерных вирусов. /Ср/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
4.3	"Защита от разрушающих программных воздействий":необходимые и достаточные условия недопущения разрушающего воздействия. /Лек/	8	2	ПК-7 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	1	
4.4	Антивирусные средства. Разворачивание ПО «Антивирус Касперского». /Лаб/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
4.5	Антивирусные средства. Разворачивание ПО «Антивирус Касперского». /Ср/	8	2	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	
4.6	/Зачёт/	8	0	ПК-7 ПК-8 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Л3.1 Э1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачету:
1.Семейство ОС Windows 2003.
2.Этапы установки Windows 2003.
3.Аппаратные требования Windows 2003.
4.Работа с дисками в Windows 2003.
5.Источники резервного питания
6.Резервное копирование данных.
7. Аппаратные устройства для разграничения доступа в сети.
8.Служба каталогов Windows 2003.
9.Домен, дерево, лес в службе каталогов Windows 2003.
10.Служба каталогов Active Directory.
11.Установка и настройка AD.
12.Управление пользователями с помощью AD.
13.Группы в AD. Типы групп.
14.Разграничение доступа к ресурсам.
15.Система безопасности Windows 2003.
16. Политика безопасности, наследование политики безопасности
17.Протокол безопасности Kerberos.
18.Firewall: назначение, принцип работы.
19.Microsoft ISA Server: особенности установки и настройки.
20.Описание протоколов VPN.
21.Компоненты VipNet
22.Secret Net назначение и функции
23.Основные особенности использования Secret Net
24.Сравнительная характеристика Proxy и Nat серверов
25.Протокол безопасности IpSec
26.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.	Программно-аппаратная защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. "Информ. безопасность"	М.: ФОРУМ, 2015	25
Л1.2	Жуковский О. И.	Информационные технологии и анализ данных: учебное пособие	Томск: Эль Контент, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Пилко И. С.	Методы информационно-аналитической деятельности. Научно-практический сборник	Кемерово: КемГУКИ, 2010	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
Л2.2	Сердюк В. А.	Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий	Москва: Издательский дом Государственного университета Высшей школы экономики, 2015	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Серпенинов О. В., Тишин В. Р.	Правовая защита информации. Словарь-глоссарий терминов в области защиты информации и информационной безопасности: для студентов спец. 090103 "Орг. и технологии защиты информ."	Ростов н/Д: Изд-во РГЭУ "РИНХ", 2010	10

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	ФСТЭК России/fstec.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
6.3.5	ПАК «Соболь».
6.3.6	ПАК «Континент».
6.3.7	Антивирус Касперского

6.4 Перечень информационных справочных систем

6.4.1	Consultant Plus

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 «11» мая 2018 г.
Зав. кафедрой _____ Тищенко Е.Н.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Технология сбора и анализа информации

Направление подготовки
10.03.01 Информационная безопасность

Профиль
10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель  Серпенинов О.В., доцент, к.т.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-7 способностью проводить анализ исходных данных для проектирования подсистемы и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений			
З. - современные достижения науки и техники в области защиты информации; общие характеристики процессов сбора, передачи, обработки и накопления информации, технических средств реализации информационных процессов.	принципы построения и организация функционирования современных устройств и систем хранения, обработки, поиска и передачи информации.	полнота и содержательность ответа умение приводить примеры	О
У. - сравнивать технико-эксплуатационные возможности устройств и систем защиты информации.	расшифровывать и проанализировать информацию о параметрах и характеристиках устройств с использованием различных источников	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. - методами контроля эффективности соответствующих проектных решений.	программно-аппаратные методы оценки и контроля эффективности соответствующих проектных решений.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

ПК-8 способностью оформлять рабочую документацию с учетом действующих нормативных и методических документов			
З.-основные руководящие, методические и нормативные документы по оформлению рабочей документации на средства обработки информации.	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям	О
У. - применять действующие нормативные и методические документы.	методы оформления результатов оценивания эффективности организации анализа и обработки информации на объектах.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. - методами оформления результатов организации анализа и обработки информации на объектах и оценки их эффективности.	Методы оформления результатов организации анализа и обработки информации на объектах и оценки их эффективности	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности			
З. - современные достижения науки и техники в области сбора и анализа информации; общие характеристики процессов сбора, передачи, обработки и накопления информации, технических средств реализации информационных	Технико-эксплуатационные показатели средств преобразования информации, используемых при обработке информации; технико-эксплуатационные показатели программно-аппаратных средств защиты информации.	полнота и содержательность ответа умение приводить примеры	О

процессов.			
У. - сравнивать технико-эксплуатационные возможности устройств и систем сбора и анализа информации.	Расшифровывать и анализировать информацию о параметрах и характеристиках устройств обработки информации с использованием различных источников	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. - методами установки, настройки и использования программно-аппаратных средства обработки информации.	Методами установки, настройки и использования программно-аппаратных средства обработки информации.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

О – опрос, ЛР- лабораторная работа

2.2 Шкалы оценивания:

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

50-100 баллов (зачет)
0-49 баллов (незачет)

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 зачету, задания для опроса, лабораторные работы.

Вопросы к зачету
по дисциплине "Технология сбора и анализа информации»
(наименование дисциплины)

1. Семейство ОС Windows 2003.
2. Этапы установки Windows 2003.
3. Аппаратные требования Windows 2003.
4. Работа с дисками в Windows 2003.
5. Источники резервного питания
6. Резервное копирование данных.
7. Аппаратные устройства для разграничения доступа в сети.

8. Служба каталогов Windows 2003.
9. Домен, дерево, лес в службе каталогов Windows 2003.
10. Служба каталогов Active Directory.
11. Установка и настройка AD.
12. Управление пользователями с помощью AD.
13. Группы в AD. Типы групп.
14. Разграничение доступа к ресурсам.
15. Система безопасности Windows 2003.
16. Политика безопасности, наследование политики безопасности
17. Протокол безопасности Kerberos.
18. Firewall: назначение, принцип работы.
19. Microsoft ISA Server: особенности установки и настройки.
20. Описание протоколов VPN.
21. Компоненты VipNet.
22. Secret Net назначение и функции.
23. Основные особенности использования Secret Net.
24. Сравнительная характеристика Proxy и Nat серверов.
25. Протокол безопасности IpSec.

Критерии оценивания:

50-100 баллов (зачет)
0-49 баллов (незачет)

Вопросы к контрольным письменным опросам

по дисциплине "Технология сбора и анализа информации»
(наименование дисциплины)

Модуль 1. «Аппаратные средства сбора информации»

КО 1. (Контрольный письменный опрос №1)

Вопросы для контрольного письменного опроса

1. Задачи сбора и анализа информации.
2. Аппаратные средства сбора информации с использованием технических каналов информации.
3. Планирование процедуры сбора информации.
4. Работа с техническими средствами обнаружения закладок.

Критерии оценивания:
- оценка «зачтено» выставляется, если ответы даны на все вопросы;
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы.

Модуль 2. «Защита данных от НСД»

КО 2. (Контрольный письменный опрос №2)

Вопросы для контрольного письменного опроса

1. Классификация подходов к защите данных от НСД.
2. Защита сетевого файлового ресурса.
3. Способы фиксации факта доступа.

4. Надежность систем ограничения доступа.
5. Сегментирование локальных сетей.
6. Стандартные способы разграничения доступа.
7. Решение проблем взаимодействия систем в процессе передачи..
8. Организация защищенного туннеля.
9. Контроль процесса передачи данных.

Критерии оценивания:
–оценка «зачтено» выставляется, если ответы даны на все вопросы;
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы.

Модуль 3. «Программно-аппаратные комплексы организации защищенного информационного обмена»

КО 3. (Контрольный письменный опрос №3)

Вопросы для контрольного письменного опроса

1. Особенности использования электронной подписи.
2. Программно-аппаратные способы шифрования..
3. Построение аппаратных компонент криптозащиты данных.
4. Методы и средства ограничения доступа к компонентам ЭВМ.
5. Организация мероприятий по контролю сетевого трафика.
6. Организация защиты данных от НСД.
7. Фиксация доступа к файлам и другим элементам ИС.
8. Порядок установки и настройки аппаратной части ПАК «Соболь».
9. Организация мероприятий по контролю сетевого трафика
10. Использование специального программного обеспечения для защиты от НСД..

Критерии оценивания:
–оценка «зачтено» выставляется, если ответы даны на все вопросы;
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы.

Модуль 4. «Защита от разрушающих программных воздействий»

КО 4. (Контрольный письменный опрос №4)

Вопросы для контрольного письменного опроса

1. Компьютерные вирусы как особый класс разрушающих программных воздействий.
2. Классификация и характеристика компьютерных вирусов.
3. Защита от разрушающих программных воздействий.
4. Необходимые и достаточные условия недопущения разрушающего воздействия.
5. Классификация и характеристика антивирусных средства.
6. Порядок разворачивания ПО «Антивирус Касперского».

Критерии оценивания:
–оценка «зачтено» выставляется, если ответы даны на все вопросы;
- оценка «не зачтено» выставляется, если ответы не даны на все вопросы.

Лабораторные работы
по дисциплине "Технология сбора и анализа информации»
(наименование дисциплины)

1. 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.

2. Критерии оценки:

«зачтено» выставляется студенту, если задание, предусмотренное лабораторной работой, выполнено на компьютере и студент может объяснить ее выполнение;

- «не зачтено» - выставляется студенту, если задание, предусмотренное лабораторной работой, не выполнено на компьютере или он не может объяснить ее выполнение.

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 зачета.

Зачет проводится по расписанию в устном виде. Количество вопросов в зачетном задании – 2. Объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную 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 № 10 от «11» мая 2018 г.
Зав. кафедрой _____ Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Технология сбора и анализа информации

Направление подготовки

10.03.01 Информационная безопасность

Профиль

10.03.01.02 Организация и технология защиты информации

Уровень образования

Бакалавриат

Составитель _____ Серпенинов О.В., доцент, к.т.н., доцент
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону
2018

Методические указания по освоению дисциплины «Технология сбора и анализа 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.