

Документ подписан простой электронной подписью.
Информация о владельце:

ФИО: Макаренко Елена Николаевна

Должность: Декан

Дата подписания: 24.04.2023 09:39:08

Уникальный программный ключ:

c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ

Директор Института магистратуры

 Иванова Е.А.

« 24 » 08 2022 г.

**Рабочая программа дисциплины
Программно-аппаратные методы защиты информации**

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования
компьютерных преступлений"

Для набора 2022 года

Квалификация
магистр


КАФЕДРА Информационные технологии и защита информации


Распределение часов дисциплины по семестрам


Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
	Неделя			
Неделя	15 2/6			
Вид занятий	уп	рп	уп	рп
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 22.02.2022 протокол № 7.

Программу составил(и): к.ф.-м.н., доцент, Карнаухов С.Н. 

Зав. кафедрой к.э.н., доц. Ефимова Е.В. 

Методическим советом направления: д.э.н., проф., Тищенко Е.Н. 

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-4:Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
ПК-1:Способен разрабатывать программно-аппаратные системы и комплексы обеспечения информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:
современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации (соотнесено с индикатором УК-4.1.) нормативно-правовые акты и методы обеспечения информационной безопасности объекта информатизации; основные разделы технического задания, методы, способы и содержание этапов проектирования и разработки программно-аппаратных систем и комплексов обеспечения информационной безопасности; технологии, методы, языки и средства программирования систем и комплексов обеспечения информационной безопасности (соотнесено с индикатором ПК-1.1.)
Уметь:
применять на практике коммуникативные технологии, методы и способы делового общения (соотнесено с индикатором УК- 4.2.) проводить сбор и анализ исходных данных для разработки, проектирования программно-аппаратных систем и комплексов обеспечения информационной безопасности с учетом нормативно-правовых актов и методических документов (соотнесено с индикатором ПК-1.2.)
Владеть:
методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств (соотнесено с индикатором УК-4.3.) навыками формирования разделов технического задания на разработку программно-аппаратных систем и комплексов обеспечения информационной безопасности; навыками проектирования и разработки программно-аппаратных систем и комплексов обеспечения информационной безопасности.(соотнесено с индикатором ПК-1.3.)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
	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/	3	6	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4

1.2	Тема 1.2 "Идентификация пользователей информационных систем-субъектов доступа к данным" Идентификация и аутентификация пользователей. Взаимная проверка подлинности. Протоколы идентификации. /Лек/	3	6	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.3	Тема 1.3 "Средства и методы ограничения доступа к ресурсам информационных систем" Защита информации от несанкционированного доступа. Система разграничения доступа к информации в компьютерных системах. Методы и средства ограничения доступа к компонентам ЭВМ. /Лек/	3	6	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.4	Тема 1.5 "Применение средств защиты информации от несанкционированного доступа для организации защищенных компьютерных систем" Методы противодействия несанкционированному доступу. Программно-аппаратные комплексы защиты информации от несанкционированного доступа /Лек/	3	6	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.5	Тема 1.4 "Организация и контроль доступа к файлам" 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. Защита файлов от изменения. /Лек/	3	8	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.6	Тема 1.2 "Идентификация пользователей информационных систем-субъектов доступа к данным" 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. LibreOffice /Лаб/	3	8	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.7	Тема 1.3 "Средства и методы ограничения доступа к ресурсам информационных систем" Ознакомление с аппаратными комплексами защиты от несанкционированного доступа к ИС. Программно-аппаратный комплекс "Соболь": ознакомление, установка, настройка. Аппаратные средства биометрической идентификации. LibreOffice /Лаб/	3	8	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.8	Тема 1.4 "Организация и контроль доступа к файлам" 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 ресурсам. /Лаб/	3	8	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.3 Л2.4
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/	3	8	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.3 Л2.4
1.10	Удаленные сетевые атаки /Ср/	3	24	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.11	Основы межсетевого взаимодействия /Ср/	3	20	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4
1.12	Зачет /Зачёт/	3	0	ПК-1 УК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Денисов, И. А.	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации	Москва: Московский технический университет связи и информатики, 2016	http://www.iprbookshop.ru/61529.html неограниченный доступ для зарегистрированных пользователей
Л1.2	Громов Ю. Ю., Иванова О. Г., Стародубов К. В., Кадыков А. А.	Программно-аппаратные средства защиты информационных систем: учебное пособие	Тамбов: Тамбовский государственный технический университет (ТГТУ), 2017	https://biblioclub.ru/index.php?page=book&id=499013 неограниченный доступ для зарегистрированных пользователей

5.2. 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		Информационная безопасность: журнал	Москва: Гротек, 2014	https://biblioclub.ru/index.php?page=book&id=364894 неограниченный доступ для зарегистрированных пользователей
Л2.3	Алакоз Г. М., Котов А. В., Курак М. В., Попов А. А., Сериков А. П.	Программно-аппаратные платформы и вычислительные наноструктуры	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428824 неограниченный доступ для зарегистрированных пользователей
Л2.4	Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: учебно-методическое пособие	Саратов: Вузское образование, 2018	http://www.iprbookshop.ru/77317.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Консультант плюс

Гарант

ФСТЭК России/fstec.ru

5.4. Перечень программного обеспечения

LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;

- персональный компьютер / ноутбук (переносной);
- проектор, экран / интерактивная доска
Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными и/или свободно распространяемыми программными средствами и выходом в Интернет.

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

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 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 (1-45) З(1-46)
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	ЛЗ (5-8) ПОЗЗ (1-5)
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	ЛЗ (5-8) ПОЗЗ (1-5)
УК-4 способен разрабатывать программно-аппаратные системы и комплексы обеспечения информационной безопасности			
З. - принципы построения и организации функционирования современных устройств и систем хранения, обработки, поиска и передачи информации;	Политика безопасности, наследование политики безопасности Протокол безопасности Kerberos. Firewall: назначение, принцип работы.	полнота и содержательность ответа умение приводить примеры	О (1-45) З(1-46)
- технико-эксплуатационные показатели средств преобразования информации, используемых при обработке экономической информации;			
У. - проектировать, планировать и разворачивать элементы комплексной системы защиты информации;	Microsoft ISA Server: особенности установки и настройки. Виды адресаций в TCP/IP сетях IP адрес: назначение, структура, применение	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-4) ПОЗЗ (1-5)
В. использования программно-аппаратных средств защиты информации в профессиональной деятельности	DNS имя: назначение, структура, применение Семиуровневая модель OSI. Характеристика стека протоколов TCP/IP.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	ЛЗ (1-4) ПОЗЗ (1-5)

З – зачет О – опрос, ЛЗ- лабораторная работа, ПОЗЗ – практико-ориентированные задания к зачету

1.2 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).

2. 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

Вопросы к зачету

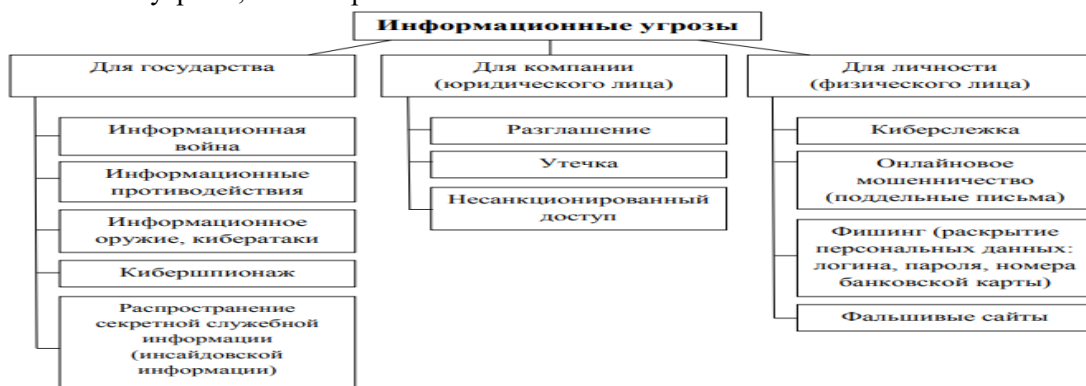
- 1) Семейство ОС Windows.
- 2) Этапы установки Windows.
- 3) Аппаратные требования Windows.
- 4) RAID. Аппаратный и программный. Типы.
- 5) RAID в Windows.
- 6) Работа с дисками в Windows.
- 7) Источники резервного питания
- 8) Резервное копирование данных.
- 9) Аппаратные устройства для разграничения 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 стека 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 Proxu и Nat серверов
- 45) Протокол безопасности IpSec
- 46) Программно-аппаратный комплекс "Соболь": назначение, установка, настройка

Практико-ориентированные задания к зачету

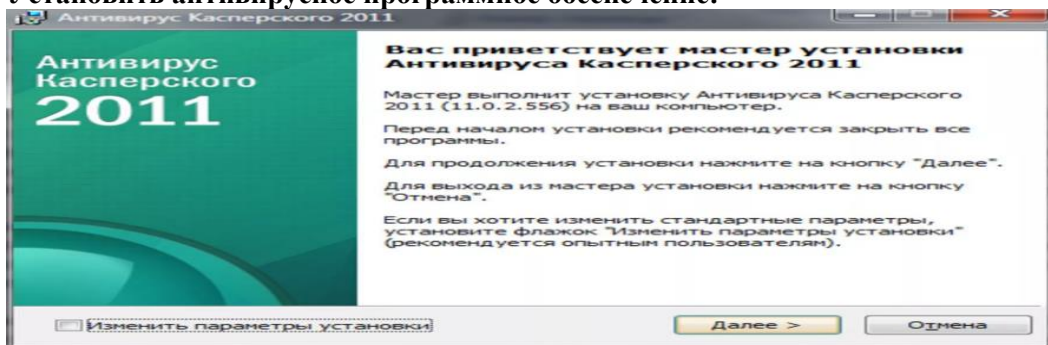
1. Установить угрозы, атаки и риски сетевой безопасности.
2. Установить антивирусное программное обеспечение.
3. Установить Linux-подобную операционную систему.
4. Настроить впервые установленную Linux-подобную операционную систему.
5. Установить шифровальную систему.

Ключ для контроля правильности выполнения практических заданий к экзамену

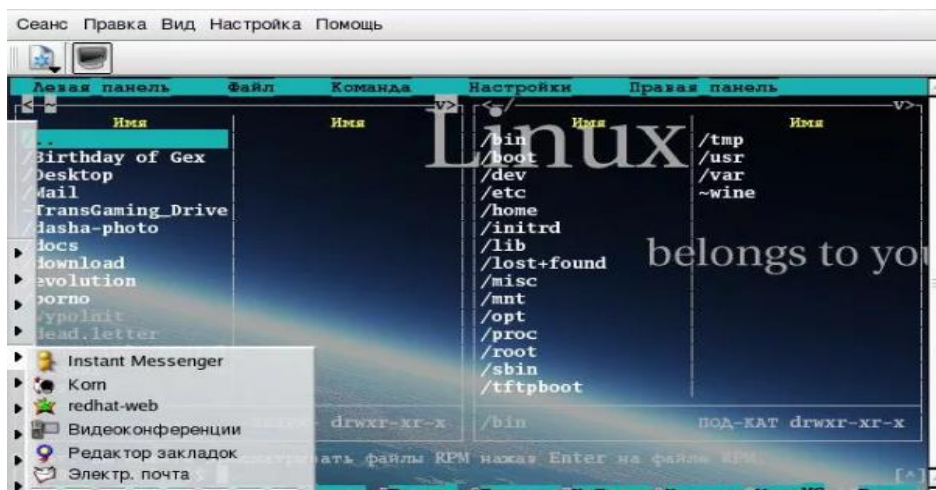
Установить угрозы, атаки и риски сетевой безопасности:



Установить антивирусное программное обеспечение:



Установить и настроить Linux-подобную операционную систему.



Установить шифровальную систему.



Критерии оценивания:

- 50-100 баллов (зачтено) – 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 (Не зачтено) – 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.

Задания для опроса

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 стека 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 Proxu и Nat серверов
45. Протокол безопасности IpSec

Критерии оценки:

- 1-20 баллов выставляется обучаемому. За один правильный ответ обучаемый получает 1 балл.

Лабораторные работы

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 ресурсам.

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.

Критерии оценки:

- (для каждого задания):

10 б. – задание выполнено верно;

9-7 б. – при выполнении задания были допущены неточности, не влияющие на результат;

6-4 б. – при выполнении задания были допущены ошибки;

3-1. – при выполнении задания были допущены существенные ошибки;

0 б. – задание не выполнено.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в

п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по окончании теоретического обучения в соответствии с расписанием. Количество вопросов в задании – 3. Объявление результатов производится в день зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

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 № _____ от _____ 28.03.2017 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, 2017

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.