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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Защита от удаленных сетевых атак

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	8			
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 25.06.2024 г. протокол № 18.

Программу составил(и): к.ф.-м.н., доц., Шейдаков Н.Е.

Зав. кафедрой: к.э.н.,доц. Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением защищенности информационных систем от удаленных сетевых атак; развитие профессиональных компетенций для нахождения оптимальных решений при построении защищенных информационных систем.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-2: способен администрировать подсистемы информационной безопасности объекта защиты

В результате освоения дисциплины обучающийся должен:

Знать:

- основные программно-технические меры и средства обеспечения информационной безопасности;
- уровни обеспечения информационной безопасности (соотнесено с индикатором ПК-2.1)

Уметь:

- проводить экспериментальные исследования защищенности объектов соответствующих физических и математических методов, - технических и программных средств обработки результатов эксперимента (соотнесено с индикатором ПК-2.2)

Владеть:

- современным программным обеспечением в области информационной безопасности;
- технической и эксплуатационной документацией на системы и средства обеспечения информационной безопасности (соотнесено с индикатором ПК-2.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Методы и средства защиты от удалённых сетевых атак

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Тема 1.1. Основные понятия в области информационной безопасности Термины и определения в области информационной безопасности. Общая классификация угроз информационной безопасности. Причины случайных воздействий. Вредоносное программное обеспечение. Компьютерные вирусы и черви. Троянские программы. Подозрительные упаковщики. Вредоносные утилиты. Угрозы безопасности сетевых информационных систем. Удаленные воздействия на сетевые информационные системы, их классификация. Отказ в обслуживании (DoS, DDoS-атаки). Формирование системы информационной безопасности / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.2	тема 1.1. Основные понятия в области информационной безопасности Основные термины в области информационной безопасности. Вредоносное ПО. Угрозы безопасности сетевых информационных систем. Формирование системы информационной безопасности. Мероприятия системы защиты информации технического характера. Механизмы защиты информации. Антивирусные средства защиты информации. Криптографические методы защиты информации. Способы предотвращения удаленных атак на информационные системы. Межсетевой экран. Прокси- сервер. Интернет- маршрутизатор. Технологии безопасности беспроводных сетей / Ср /	8	10	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.3	Тема 1.1. «Изучение системы обнаружения атак Snort» Получение навыков работы с программой Snort, изучение принципов создания правил обработки трафика. Основные сведения о системе обнаружения атак Snort. /LibreOffice / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.4	Тема 1.2. Механизмы защиты информации. Программно-аппаратные средства обеспечения безопасности информационных сетей. Механизмы защиты информации. Антивирусные средства защиты информации. Криптографические методы защиты информации. Симметричное шифрование. Асимметричное шифрование. Сертификаты открытых ключей. Защита от атаки "анализ сетевого трафика". Программно-аппаратные средства	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

	обеспечения безопасности информационных сетей. Межсетевой экран. Фильтрация на сетевом уровне. Фильтрация на прикладном уровне. Прокси-сервер Интернет-маршрутизатор. / Лек /				
1.5	Тема 1.3. Технологии безопасности беспроводных сетей Технологии безопасности беспроводных сетей. Комплексная система обеспечения безопасности беспроводных сетей. Стандарт IEEE 802.1x/EAP. Развертывание беспроводных виртуальных сетей. Системы обнаружения вторжения в беспроводных сетях. Унифицированные решения / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
1.6	Тема 1.1. “Сканер портов Nmap” Ознакомление с различными типами сканеров портов и принципами их работы; изучить основные методы сканирования для достижения максимальной эффективности; изучить работу Nmap – свободной утилиты, предназначенной для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов и определения состояния объектов сканируемой сети (портов и соответствующих им служб). /LibreOffice / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

Раздел 2. Аппаратные и программные технологии защиты от сетевых атак

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Тема 2.1. Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизаторах. Протоколы и функции, обеспечивающие работу сети. Маршрутизация. Протокол OSPF. Терминология протокола OSPF. DHCP-клиент в межсетевых экранах. DHCP-сервер в межсетевых экранах. Функция DHCP Relays в межсетевых экранах. Сервисы DNS. Резервирование маршрутов (Route Failover). Балансировка нагрузки сети. Использование метрик маршрута с алгоритмом Round Robin. Использование метрик маршрута с алгоритмом Spillover. / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.2	Тема 2.1. «Изучение программного пакета анализа сетевого трафика Wireshark» Получение навыков анализа протоколов с помощью программного обеспечения Wireshark. Фильтры Wireshark. Анализ трафика Wireshark. Составление отчёта о состоянии портов. /LibreOffice / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.3	Тема 2.1. Организационные и аппаратные меры защиты ОС. Программные и аппаратные механизмы защиты. Классификация угроз безопасности ОС. Типичные атаки на ОС. Понятие защищенной операционной системы. Подходы к построению защищенных ОС: фрагментарный и комплексный. Административные меры защиты. Адекватная политика безопасности. / Ср /	8	16	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.4	Тема 2.2. Протоколы IGMP и UPnP. Качество обслуживания и Технология SharePort. IGMaP для IPTV. Что такое IPTV. Поддержка UPnP. Качество обслуживания (QoS) и управление полосой пропускания трафика (Traffic Shaping). Межсетевые экраны для управления полосой пропускания трафика. Использование технологии QoS в Интернет-маршрутизаторах. Технология SharePort. / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.5	Тема 2.2. Работа с системой анализа защищенности XSpider 7.0. Создание профиля для сканирования уязвимостей ОС Linux, выполнение сканирования и генерация отчета о выполненной работе. Создание профиля для сканирования уязвимостей. Поиск уязвимостей ОС. Просмотр и исправление обнаруженных уязвимостей. /LibreOffice / Лаб /	8	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.6	2.3. Фильтрация трафика и виртуальные сети. Фильтрация трафика. Виртуальные локальные сети VLAN. Виртуальные частные сети (VPN). Протокол PPTP. Как происходит установление соединения PPTP? Протокол L2TP. Набор протоколов IPSec. Компоненты IPSec. Установка и поддержка VPN. Dead Peer Detection. Протокол NAT Traversal. Использование ключей (Pre-Shared Key). L2TP over IPSec. /LibreOffice / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.7	Тема 2.3. Организация ARP-spoofing'a с помощью Ettercap.	8	6	ПК-2	Л1.1, Л1.2, Л1.3,

	Ettercap - сниффер для коммутируемых локальных сетей. Организовать прослушивание трафика между двумя хостами, соединёнными между собой с помощью коммутируемой сети. Просмотр результатов атаки. Изучение результатов работы tcpdump. /LibreOffice / Лаб /				Л1.4, Л2.1, Л2.2, Л2.3
2.8	Тема 2.3. Построение защищенных виртуальных сетей Способы создания защищенных виртуальных каналов. Обзор протоколов. Канальный уровень модели OSI. Сетевой уровень модели OSI. Сеансовый уровень модели OSI. Туннелирование на канальном уровне. Протокол PPTP. Протокол L2F. Протокол инкапсулирующей защиты содержимого. Управление защищенным туннелем. / Ср /	8	18	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.9	Тема 2.4. Виртуальные частные сети. IPSec-туннель. Изучение защищенного IPSec-туннеля и способа его настройки на брандмауэре ASA5505 и в ОС Linux. Криптографические методы: VPN, туннелирование. /LibreOffice / Лаб /	8	2	ПК-2	Л1.1, Л1.3, Л2.1, Л2.3
2.10	Тема 2.4. Функции IDP, WCF, AV и технология ZoneDefense. Функции IDP, WCF, AV. Обнаружение вторжений (Intrusion Detection). Компоненты NetDefendOS IDP. Правила IDP (IDP Rules). Компоненты правил. IDP-поиск соответствия с образцом (IDP Pattern Matching). Обновление в HA-кластере. Фильтрация Web-содержимого (WCF). Технология ZoneDefense. Компоненты SNMP. Безопасность SNMP. Пороговые правила (Threshold Rules). ZoneDefense и сканирование антивирусом. / Лек /	8	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3
2.11	Тема 2.5. Особенности применения межсетевых экранов и маршрутизаторов. Общие характеристики Интернет-маршрутизаторов. Интернет-маршрутизаторы для малых офисов и рабочих групп. Широкополосный маршрутизатор. Коммутатор VLAN. Интернет-маршрутизаторы серии Unified Services. Маршрутизаторы ADSL Обзор межсетевых экранов NetDefend D-Link. / Лек /	8	4	ПК-2	Л1.1, Л1.3, Л2.1, Л2.3
2.12	Зачёт / Зачёт /	8	0	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л2.1, Л2.2, Л2.3

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,	Заглавие	Издательство, год	Колич-во
Л1.1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.2	Сердюк В. А.	Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие	Москва: Издательский дом Высшей школы экономики, 2015	http://biblioclub.ru/index.php?page=book&id=440285 неограниченный доступ для зарегистрированных пользователей
Л1.3	Голиков А. М.	Защита информации в инфокоммуникационных системах и сетях: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015	https://biblioclub.ru/index.php?page=book&id=480637 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.4	Руденков, Н. А., Пролетарский, А. В., Смирнова, Е. В., Суровов, А. М.	Технологии защиты информации в компьютерных сетях	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/73732.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2014	https://biblioclub.ru/index.php?page=book&id=238445 неограниченный доступ для зарегистрированных пользователей
Л2.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	https://biblioclub.ru/index.php?page=book&id=438331 неограниченный доступ для зарегистрированных пользователей
Л2.3	Прохорова, О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014	https://www.iprbookshop.ru/43183.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Официальный сайт ФСТЭК России: www.fstec.ru, раздел "Техническая защита информации"
ScienceDirect. https://www.sciencedirect.com/
КонсультантПлюс

5.4. Перечень программного обеспечения

Операционная система РЕД ОС
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

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 программными средствами и выходом в Интернет.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

Приложение 1

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-2: способен администрировать подсистемы информационной безопасности объекта защиты			
З - основные программно-технические меры и средства обеспечения информационной безопасности; - уровни обеспечения информационной безопасности;	поиск и сбор необходимой литературы, использование современных информационно- коммуникационных технологий и глобальных информационных ресурсов для подготовки к зачету, опросу	полнота и содержательность ответа на зачете, опросе	*З (1-33)* *О* (1-20)
У. - проводить экспериментальные исследования защищенности объектов соответствующих физических и математических методов, - технических и программных средств обработки результатов эксперимента	решение тематических з по соответствующим разделам курса; выполнение лабораторных и практико-ориентированных заданий	объем выполненных работы (в полном, не полном объеме)	ПОЗЗ (1-9) ЛЗ (1-6)
В. - современным программным обеспечением в области информационной безопасности; - технической и эксплуатационной документацией на системы и средства обеспечения информационной безопасности;	выбирает современное программное обеспечение при выполнении лабораторных и практико-ориентированных заданий	правильный выбор программного обеспечения для выполнения лабораторных и практико-ориентированных заданий	ПОЗЗ (1-9) ЛЗ (1-6)

О – опрос, З – вопросы для зачета, ПОЗЗ – практико-ориентированные задания для зачета, ЛЗ – лабораторные задания

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. Основные понятия информационной безопасности.
2. Основные составляющие. Доступность, целостность и конфиденциальность информации.
3. Доктрина информационной безопасности РФ.
4. Классификация защищаемой информации по степени важности и ценности.
5. Основные определения и критерии классификации угроз.
6. Законодательный уровень информационной безопасности.
7. Административный уровень информационной безопасности.
8. Содержание политики безопасности. Программа безопасности.
9. Управление рисками. Основные понятия. Подготовительный этап управления рисками.
10. Управление рисками. Основные этапы управления рисками.
11. Методы и модели анализа угроз.
12. Поддержание работоспособности. Реагирование на нарушения режима безопасности.
13. Основные программно-технические меры.
14. Архитектурная безопасность.
15. Идентификация и аутентификация, управление доступом.

16. Мониторинг и аудит.
17. Шифрование, контроль целостности.
18. Экранирование, анализ защищенности.
19. Классификация межсетевых экранов.
20. Основные причины возможности проведения атаки типа Инъекция.
21. Алгоритм поведения атаки типа Иньекиия на скрипт-коды.
22. Алгоритм проведения атаки типа SQL-инъекция
23. Классификация XSS атак.
24. Отличия между хранимой и временной XSS атаками.
25. Понятия и сущность Flood-атаки.
26. Различия между DoS и DDoS атаками.
27. Методы проведения DNS-атак.
28. Методы проведения атаки BruteForce.
29. Условия успешного проведения атак типа DoS/DDoS/Flood.
30 Причины актуальности сетевых удаленных атак.
31. Сущность активного сканирования атакуемого сетевого ресурса.
32. Сущность пассивного сканирования атакуемого сетевого ресурса.
33. Методы анализа атакуемого узла.

Практико-ориентированные задания к зачету

1. Формирование модели нарушителя компьютерных сетей.
2. Анализ средств противодействия компьютерным атакам.
3. Механизмы защиты информации.
4. Основы мониторинга информационной безопасности.
5. Фильтрация трафика и виртуальные сети. Технология преобразования сетевых адресов, механизмы.
6. Механизмы защиты информации.
7. Управление межсетевыми экранами.
8. Управление системой анализа.
9. Источники сбора информации. Выбор источников информации.

Критерии оценивания:

- 84-100 баллов (оценка «зачет») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированных заданий, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 0-49 баллов (оценка «незачет») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять умения и навыки при решении практико-ориентированных заданий, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Вопросы для опросов

1. Определение статического метода анализа исполняемого кода
2. Определение динамического метода анализа исполняемого кода
3. Параметры воздействия сетевой атаки на внешний периметр информационной системы
4. Параметры воздействия сетевой атаки на внутренний периметр информационной системы
5. Этапы проведения сетевой атаки.
6. Определение самого сложного по реализации этапа сетевой атаки
7. Цели сетевой удаленной атаки.
8. Методы анализа атакуемого узла.
9. Классификация удаленных атак по уровню воздействия на атакуемые объекты
10. Сущность атаки типа Sniffing.
11. Сущность атаки типа Spoofing.
12. Алгоритм проведения атаки типа SQL-инъекция
13. Классификация XSS атак.
14. Понятия и сущность Flood-атаки.
15. Различия между DoS и DDoS атаками.
16. Методы проведения DNS-атак.
17. Условия успешного проведения атак типа DoS/DDoS/Flood.

18. Причины актуальности сетевых удаленных атак.
19. Сущность активного сканирования атакуемого сетевого ресурса.
20. Сущность пассивного сканирования атакуемого сетевого ресурса.

Примечание: опрос проводится при проверке всех лабораторных заданий для выявления знаний при изучении соответствующих тем дисциплины в рамках текущей аттестации.

Критерии оценивания:

- 2 балла выставляется обучающемуся, если изложенный материал фактически верен и логически обоснован.
- 1 балл выставляется обучающемуся, если изложенный материал фактически верен, но есть незначительные ошибки.
- 0 баллов, если ответ не верен

Максимальное количество баллов за семестр – **40 баллов**.

Лабораторные задания

Лабораторное задание 1. «Изучение системы обнаружения атак Snort»

Получение навыков работы с программой Snort, изучение принципов создания правил обработки трафика. Основные сведения о системе обнаружения атак Snort.

Лабораторное задание 2. . “Сканер портов Nmap”

Ознакомление с различными типами сканеров портов и принципами их работы; изучить основные методы сканирования для достижения максимальной эффективности; изучить работу Nmap – свободной утилиты, предназначенной для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов и определения состояния объектов сканируемой сети (портов и соответствующих им служб

Лабораторное задание 3. «Изучение программного пакета анализа сетевого трафика Wireshark»

Получение навыков анализа протоколов с помощью программного обеспечения Wireshark. Фильтры Wireshark. Анализ трафика Wireshark. Составление отчёта о состоянии портов

Лабораторное задание 4. Работа с системой анализа защищенности XSpider 7.0.

Создание профиля для сканирования уязвимостей ОС Windows и ОС Linux, выполнение сканирования и генерация отчета о выполненной работе. Создание профиля для сканирования уязвимостей. Поиск уязвимостей ОС. Просмотр и исправление обнаруженных уязвимостей.

Лабораторное задание 5. . Организация ARP-spoofing'а с помощью Ettercap.

Ettercap - сниффер для коммутируемых локальных сетей. Организовать прослушивание трафика между двумя хостами, соединёнными между собой с помощью коммутируемой сети. Просмотр результатов атаки. Изучение результатов работы tcpdump.

Лабораторное задание 6. Виртуальные частные сети. IPSec-туннель.

Изучение защищенного IPSec-туннеля и способа его настройки на брандмауэре ASA5505 и в ОС Linux. Криптографические методы: VPN, туннелирование.

Критерии оценивания:

- (для каждого задания):

10 баллов – задание выполнено верно;
9-7 баллов – при выполнении задания были допущены неточности, не влияющие на результат;
6-3 балла – при выполнении задания были допущены ошибки;
2 - 1 балл – при выполнении задания были допущены существенные ошибки;
0 баллов – задание не выполнено.

Максимальное количество баллов за семестр **60 баллов**.

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 расписанию промежуточной аттестации в виде опросов. Количество вопросов – 3. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В ходе лекционных занятий рассматриваются теоретические вопросы с учетом практико-ориентированности изучаемой дисциплины, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки работы с компьютером, применения методов и технологий защиты информации.

При подготовке к лабораторным занятиям каждый обучающийся должен:

– изучить рекомендованную учебную литературу;

– изучить практические примеры, рассмотренные на лекциях;

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

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

Студент должен готовиться к предстоящему лабораторному занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.