Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ
Проректор по учебной работе
_____ С.Ю. Рубцова
(подпись, расшифровка подписи)
"__" _____ 2019 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.В.ДВ.09.02 Сетевая безопасность

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
01.03.02 Прикладная математика и информатика

профиль
Системное программирование и компьютерные технологии

Квалификация
бакалавр

Форма обучения
очная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2019 г.

Рабочая программа дисциплины Б1.В.ДВ.09.02 Сетевая безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.02 Прикладная математика и информатика.

Программу составил(и):

Е.Н. Козлов, старший преподаватель кафедры информатики

Рабочая программа дисциплины Б1.В.ДВ.09.02 Сетевая безопасность утверждена на заседании кафедры информатики, протокол № 8 от 02 апреля 2019 г.

Заведующий кафедрой Г.С. Осипов

Рецензент:
А.В. Лоскутов,
ведущий научный сотрудник лаборатории цунами Института морской геологии и геофизики Дальневосточного отделения Российской академии наук, к.ф.-м.н.

1. Цель и задачи дисциплины

Цель дисциплины

Целью изучения дисциплины является предоставление обучаемым знаний об основных типах и способах защиты информации в компьютерных сетях, а также навыков по проектированию системы защиты информации и анализу защищенности вычислительных сетей.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных принципов информационной безопасности сетевого оборудования;
- ознакомление с техническими и технологическими решениями, используемыми в данной области;
- выработка практических навыков аналитического и экспериментального исследования основных методов и средств, используемых в области, изучаемой в рамках данной дисциплины.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Сетевая безопасность» относится к части по выбору Блока 1 Дисциплины (модули) (Б1.В.ДВ.09.02) подготовки студентов по направлению подготовки бакалавров 01.03.02 «Прикладная математика и информатика».

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знании следующих дисциплин: Теоретические основы информатики; Операционные системы; Компьютерные сети.

Постреквизиты дисциплины:

Основные положения данной дисциплины выступают опорой для подготовки к прохождению учебной, производственной и преддипломной практик, к научно-исследовательской работе.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПКС-1	Способен разрабатывать, изменять и согласовывать архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения	ПКС-1.1 Знать существующие архитектуры программного обеспечения. ПКС -1.2 Уметь использовать существующие архитектуры программного обеспечения. ПКС-1.3 Иметь навыки разработки и программного обеспечения различных архитектур.
ПКС-4	Способен проектировать программные интерфейсы	ПКС-4.1 Знать основные принципы проектирования программных интерфейсов. ПКС -4.2 Уметь использовать принципы проектирования программных интерфейсов. ПКС-4.3 Иметь навыки проектирования программных интерфейсов.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет ***2*** зачетные единицы (***72*** академических часа).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	8	
Общая трудоемкость	**72**	**72**
Контактная работа:	**52**	**52**
Лекции (Лек)	24	**24**
Лабораторные работы (Лаб)	24	**24**
Контактная работа в период теоретического обучения (КонтТО) *(Проведение текущих консультаций и индивидуальная работа со студентами)*	4	**4**
Контактная работа в период промежуточной аттестации (КонтПА)		
Промежуточная аттестация *зачет*		
Самостоятельная работа:	20	**20**
	20	**20**
- *самостоятельное изучение разделов (перечислить);*	2	**2**
- *самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);*	6	**6**
- *подготовка к лабораторным занятиям;*	8	**8**
- *подготовка к промежуточной аттестации и т.п.)*	4	**4**

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

Очная форма обучения

№ п/п	Раздел дисциплины/ темы		Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
			контактная			Самостоятельная работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
8 семестр							
1.	Тема 1. Виды атак. Модель сетевой безопасности.	**8**	2	0	2	2	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Тема 2. Криптография и системы шифрования.		4	0	2	2	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Тема 3. Механизмы обеспечения безопасности коммутируемых локальных сетей.		4	0	4	2	Устный опрос по теме лекции. Проверка домашнего задания.
4.	Тема 4. Механизмы обеспечения безопасности беспроводных локальных сетей.		4	0	4	2	Устный опрос по теме лекции. Проверка домашнего задания.
5.	Тема 5. Механизмы межсетевой безопасности.		4		4	2	Устный опрос по теме лекции. Проверка домашнего задания.
6.	Тема 6. Системы тунелирования.		4		4	2	Устный опрос по теме лекции.

							Проверка домашнего задания.
7.	Тема 7. Безопасность удаленного управления.		2		4	4	Устный опрос по теме лекции. Проверка домашнего задания.
	зачет					4	*Устный зачет*
	итого:	**104**	**24**	**0**	**24**	**20**	

4.3.Содержание разделов дисциплины

7 семестр

Тема 1. Виды атак. Модель сетевой безопасности

Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Взлом целевой системы. Сокрытие следов взлома. Классификация атак. Модель сетевой безопасности.

Тема 2. Криптография и системы шифрования.

Криптография. Структура шифрования Фейстеля. Алгоритмы стандартного шифрования. Режимы работы блочных шифровальщиков. Расположение устройств шифрования. Распределение ключей. Криптография и аутентификация сообщений на основе общего ключа.

Тема 3. Механизмы обеспечения безопасности коммутируемых локальных сетей.

Ограничение количества управляющих компьютеров. Настройка безопасности индивидуального порта. Фильтрация MAC-адресов. Технология фильтрации IP-MAC Binding. Списки контроля доступа. Сегментация трафика. Протокол IEEE 802.1x. Виртуальные сети. Аудит безопасности протокола связующего дерева STP.

Тема 4. Механизмы обеспечения безопасности беспроводных локальных сетей.

Классификация механизмов безопасности в сетях Wi-Fi. Механизмы шифрования. Принцип аутентификации абонента. Открытая аутентификация. Аутентификация с общим ключом. Аутентификация по MAC-адресу. Дополнительные механизмы защиты.

Тема 5. Механизмы межсетевой безопасности.

Межсетевые экраны. Фильтры пакетов. Фильтры инспекции состояний. Транслятор адресов. Транспортные шлюзы. Шлюзы приложений. Системы обнаружения атак и вторжений.

Тема 6. Системы тунелирования.

Протокол PPPoE. Виртуальные частные сети. Протокол IPSEC. Протокол SSL/TLS.

Тема 7. Безопасность удаленного управления.

Аудит безопасности протокола SNMP. Версии протокола SNMP. Протокол SNMPv3. Протокол SSH. Рекомендации по безопасности использования протокола SSH.

4.4 Темы и планы лабораторных занятий

8 семестр

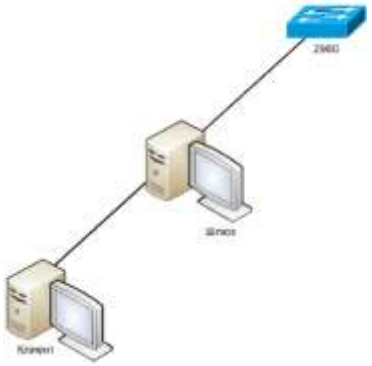
1) **Аудит безопасности протокола SNMP:**

   Цель работы:

   Изучение способов мониторинга и управления сетью на основе протокола SNMP с использованием собственных механизмов безопасности.

   Порядок выполнения работы:

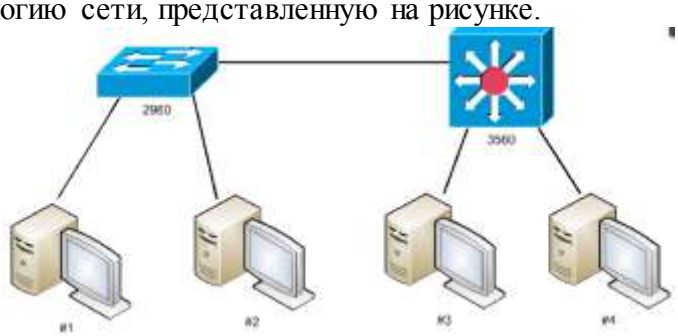
   1. Постройте топологию сети, показанную на рисунке



2. Настройте маршрутизацию между сетями.
3. Настройте SNMP-протокол на коммутаторе.
4. На Шлюзе запустите tcpdump. Отсеивайте из потока только пакеты протокола SNMP.
5. Запустите утилиту iReasoning MIB Browser.
6. Загрузите базу MIB RFC-1213.
7. С Клиента на коммутаторе выясните следующие параметры: • название устройства, время работы устройства, службы, запущенные на устройстве (ветвь system);
• количество интерфейсов на устройстве, содержимое таблицы интерфейсов, назначение двух дополнительных виртуальных портов (ветвь interfaces);
• IP-адрес устройства, содержимое таблицы маршрутизации (ветвь ip);
• TCP-соединения, установленные устройством (ветвь tcp).
8. Выясните из перехваченных на шлюзе пакетов SNMP Community String.
9. Со Шлюза выясните состояние портов коммутатора.
10. Сделайте вывод о безопасности протоколов SNMP v1/v2c, границах их применимости и предложите методы защиты этих протоколов.

2) Виртуальные локальные сети IEEE 802.1q:

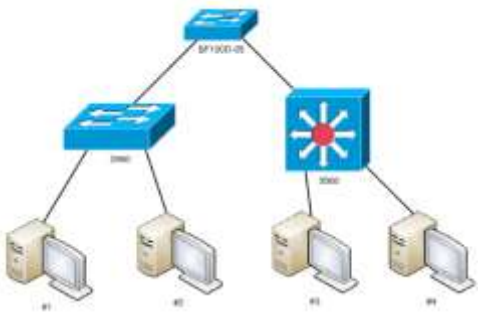
Цель работы:
Изучение технологий виртуальных сетей. Получение навыков настройки VLAN на основе тэгов IEEE 802.1q в сети, построенной на коммутаторах Cisco.
Порядок выполнения работы:
1. Постройте топологию сети, представленную на рисунке.



2. Сконфигурируйте VLAN на основе тегов таким образом, чтобы рабочие станции 1 и 4 принадлежали виртуальной сети №1, станция 2 принадлежала виртуальной сети №2, а станция №3 – виртуальной сети №3 и при этом являлась общедоступным ресурсом. То есть машины в виртуальных сетях №1 и №2 не должны взаимодействовать между собой, но должны взаимодействовать с машиной №3.
3. Проверьте правильность конфигурации сети. Результаты мониторинга покажите и поясните преподавателю.
4. Сбросьте настройки коммутаторов в фабричные и перезагрузите его.

3) Базовые механизмы безопасности коммутаторов:

Цель работы:
Изучение технологий Trusted Hosts, IP-MAC Binding и Port Security.
Порядок выполнения работы:
1. Соберите топологию сети, представленную на рисунке.



2. Настройте коммутаторы таким образом, чтобы ими могли управлять только машины #1 и #3.
3. Проверьте выполненные настройки.
4. Очистите таблицы коммутации на всех коммутаторах.
5. С машин #1 и #2 «пропингуйте» машину #3.
6. Убедитесь, что в таблицах коммутации не присутствует аппаратного адреса машины #4.
7. Заблокируйте на обоих коммутаторах таблицу коммутации в режиме Permanent.
8. Попытайтесь осуществить взаимодействие с 4-ым компьютером с любого компьютера. Объясните полученный результат.
9. Сбросьте блокировку таблиц коммутации.
10. Используя технологию IP-MAC Binding, настройте на коммутаторах фильтры таким образом, чтобы в сети могли работать только машины #1 и #3.
11. Сбросьте настройки коммутаторов в фабричные и перезагрузите его.

4) Безопасность на основе протокола IEEE 802.1x:

Цель работы:
Изучение протокола IEEE 802.1x, способов его настройки на сетевых узлах, способов настройки сервера RADIUS.
Порядок выполнения работы:
1. Соберите сеть с топологией, представленной на рисунке 1.

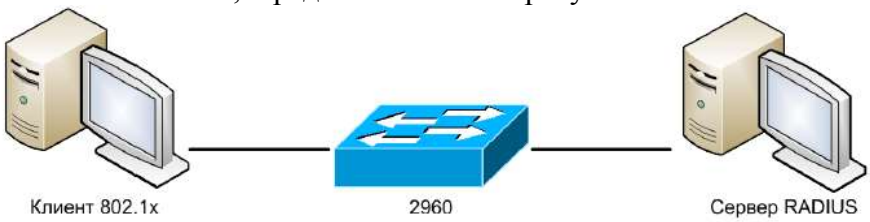


Рисунок 1. Топология коммутируемой сети.

2. Настройте сервер RADIUS, используя утилиту *freeradius*.
3. Включите протокол 802.1x на коммутаторе. Используйте авторизацию на основе портов.
4. Переведите порт коммутатора, к которому подключен клиент 802.1x, в неавторизованное состояние.
5. Настройте клиента 802.1x, используя утилиту *wpa_supplicant*.
6. Запустите клиента 802.1x.
7. Проверьте успешность авторизации порта путём:
• взаимодействия между машинами;
• анализа журнала (логов) клиента 802.1x;
• анализа журнала сервера.
8. Физически отключите кабель клиента от порта коммутатора, а затем заново подключите. Выясните, в каком состоянии (авторизации) находится порт клиента. Ответьте на вопрос, можно ли нарушить безопасность сети путём физического подключения неавторизованной машины на авторизованный порт коммутатора.
9. Соберите сеть с топологией, представленной на рисунке 2.

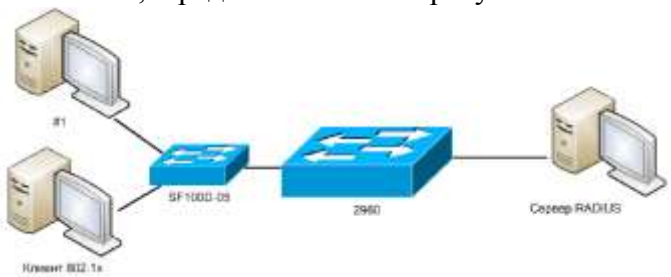


Рисунок 2. Топология коммутируемой сети.

10. Авторизуйте порт коммутатора 2960, используя клиента 802.1x.
11. Попробуйте осуществить взаимодействие машины № 1 и сервера RADIUS. Какие выводы можно сделать об уязвимостях в безопасности протокола 802.1x на основе портов.
12. Соберите сеть с топологией, представленной на рисунке 3.

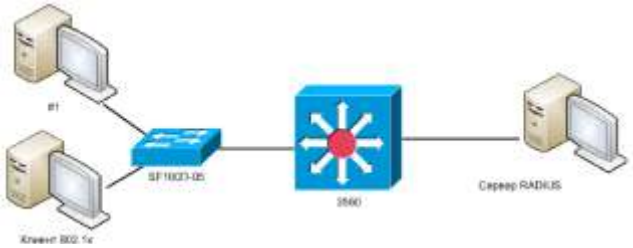


Рисунок 3. Топология коммутируемой сети.

13. Включите протокол 802.1x на коммутаторе. Используйте авторизацию на основе MAC-адресов.
14. Переведите порт коммутатора 3560, к которому подключен коммутатор SD205, в неавторизованное состояние. Затем инициируйте данный порт MAC-адресом машины, на которой запущен клиент 802.1x.
15. Запустите клиента 802.1x.
16. Проверьте успешность авторизации порта путём:
• взаимодействия между клиентом и сервером;
• анализа журнала (логов) клиента 802.1x;
• анализа журнала сервера.
17. Попробуйте осуществить взаимодействие между машиной № 1 и сервером.
18. Настройте и запустите клиента 802.1x на машине № 1. Теперь попробуйте осуществить взаимодействие между машиной № 1 и сервером. На основе полученных результатов сделайте вывод о защищенности протокола 802.1x на основе MAC-адресов.
19. Сбросьте настройки коммутатора в фабричные и перезагрузите его.

5. Темы дисциплины (модуля) для самостоятельного изучения

8 семестр (2 ч.)

№	Название темы	Количество часов
1.	Использование современных технологий для взлома компьютерных сетей.	2

Вопросы для самоконтроля:

1. Перечислите современные способы взлома компьютерных сетей.
2. Опишите алгоритм использования облачных технологий в качестве инструмента взлома.
3. Опишите риски, связанные с разработкой квантовых компьютеров.

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
	8 семестр		
1.	Тема 1. Виды атак. Модель сетевой	Лекция	Традиционная лекция в ауд. с мультимедиа проектором

	безопасности.	Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Тема 2. Криптография и системы шифрования.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Тема 3. Механизмы обеспечения безопасности коммутируемых локальных сетей.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
4.	Тема 4. Механизмы обеспечения безопасности беспроводных локальных сетей.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
5.	Тема 5. Механизмы межсетевой безопасности.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
6.	Тема 6. Системы тунелирования.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
7.	Тема 7. Безопасность удаленного управления.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Примерный вариант контроля знаний по различным темам

1. Каким образом TKIP обеспечивает более высокий уровень защиты для среды WLAN?
   - Он использует алгоритм AES
   - Он уменьшает размер вектора инициализации (IV) и использует алгоритм AES
   - Он использует дополнительный ключевой материал
   - Он использует фильтрацию по MAC и IP

2. Что из перечисленного ниже не является характеристикой стандарта IEEE 802.11a?
   - Он работает в диапазоне 5 ГГц

- Он использует технологию расширения спектра OFMD
- Он обеспечивает пропускную способность 52 Мбит/с
- Он покрывает меньшую площадь по сравнению с 802.11b

3. Что может быть использовано для обхода функции обратного вызова?
- Пассивное прослушивание телефонных разговоров (wiretapping)
- Переадресация вызовов
- Спуфинг пакетов
- Брутфорс-атака

4. Что не считается компонентом архитектуры межсетевого экрана, используемым для защиты сетей?
- Экранированный узел
- Экранированная подсеть
- Шлюз NAT
- Двухуровневая DMZ

5. Почему коммутируемая среда более безопасна, чем маршрутизируемая?
- В ней сложнее перехватывать трафик с помощью сниффера, поскольку компьютеры работают через выделенные виртуальные соединения
- Она также небезопасна, как и некоммутируемые среды
- Шифрование на канальном уровне не позволяет перехватывать передаваемую информацию
- Коммутаторы являются более интеллектуальными устройствами по сравнению с мостами, и они содержат механизмы безопасности

6. Какой из указанных ниже протоколов выполняет предварительное установление соединения?
- IP
- ICMP
- UDP
- TCP

7. Что из перечисленного ниже лучше всего описывает передачу трафика Ethernet через локальную сеть (LAN)?
- Трафик направляется шлюзу, который посылает его системе получателя
- Трафик хаотичен по своей природе, осуществляется его широковещательная передача всем узлам в подсети
- Трафик передается в виде потока, широковещательная передача данных не производится
- Трафик остается в пределах коллизионного, но не широковещательного домена

8. Какой из перечисленных ниже прокси не может принимать решение о доступе на основе команд протоколов?
- Прикладного уровня
- С фильтрацией пакетов
- Сетевого уровня
- С контролем состояния

9. Какая проблема безопасности часто присутствует в распределенных средах и системах?
- Неизвестны правильные адреса прокси и шлюза по умолчанию
- Неизвестно, кому можно доверять
- Неизвестен наиболее предпочтительный метод аутентификации

- Неизвестно, каким образом преобразовывать имена узлов

10. Что является другим названием VPN?
    - Транспортный сеанс
    - Туннель
    - Сквозное (end-to-end) соединение
    - Полоса пропускания

Форма контроля (8 семестр) – ***зачет***

Примерные вопросы к зачету (8 семестр)

1. Классификация сетевых атак.
2. Модели сетевой безопасности.
3. Стандартные алгоритмы шифрования.
4. Криптография, криптоанализ.
5. Режимы работы блочных шифровальщиков.
6. Криптография и аутентификация на основе общего ключа.
7. Ограничение количества управляющих компьютеров.
8. Настройка безопасности индивидуального порта. Фильтрация MAC-адресов. Технология фильтрации IP-MAC Binding.
9. Списки контроля доступа. Сегментация трафика.
10. Протокол IEEE 802.1x. Роли устройств. Процесс аутентификации.
11. Виртуальные сети. Сети на базе MAC-адресов.
12. Виртуальные сети. Сети на базе портов.
13. Виртуальные сети. Сети на базе маркированных кадров.
14. Аудит безопасности протокола связующего дерева STP.
15. Возможные схемы атак при использовании STP.
16. Классификация механизмов безопасности в сетях Wi-Fi.
17. Механизмы шифрования.
18. Межсетевые экраны. Архитектура межсетевого экрана.
19. Межсетевые экраны. Транслятор адресов.
20. Межсетевые экраны. Шлюзы приложений.
21. Системы обнаружения атак и вторжений.
22. Системы тунелирования. Протокол PPPoE.
23. Виртуальные частные сети. Протоколы PPTP и L2TP.
24. Виртуальные частные сети. Протоколы IPSEC.
25. Безопасность удаленного управления.

8. Система оценивания планируемых результатов обучения

Критерии оценивания

Критерием оценивания является выполнение самостоятельных заданий и лабораторных работ.

Самостоятельные задания и лабораторные работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров:

– своевременное выполнение работы;

– полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий, студент имеет возможность сдавать теоретический зачет по вопросам.

– оценка «зачтено» выставляется студенту, который твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

оценка «не зачтено» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в

ответе или в решении задач грубые ошибки.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	*0,25*	*0,5*	9	18
Выполнение домашнего задания	*0,75*	*0,75*	27	27
Выполнение заданий самостоятельной работы	*1*	*3*	4	12
Промежуточная аттестация (зачет)			*20*	*43*
Итого за семестр */зачет*			*60*	*100*

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. Практикум по дисциплине Сетевая безопасность и ее планирование [Электронный ресурс]/ — Электрон. текстовые данные.— Москва: Московский технический университет связи и информатики, 2016.— 28 с.— Режим доступа: http://www.iprbookshop.ru/61540.html.— ЭБС «IPRbooks»
2. Басыня, Е. А. Сетевая информационная безопасность и анонимизация : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2016. — 76 с. — ISBN 978-5-7782-3107-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91519.html.
3. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77317.html

9.2.Дополнительная литература

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/ В.Ф. Шаньгин – Москва: ДМК Пресс, 2014
2. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/Б.А. Фороузан – Москва: ИУИТ, 2014
3. Магомедов М.С. Учебное пособие по дисциплине «Безопасность вычислительных сетей» для направления подготовки «Информационная безопасность» /М.С. Магомедов - Махачкала.: изд. «Формат», 2015
4. Иванова М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванова – Москва: МИФИ, 2014.
5. Щербаков В.Б. Безопасность беспроводных сетей: стандарт IEEE 802.11/ В.Б. Щербаков, С.А. Ермаков - М: РадиоСофт – 2014 – 255с.
6. Таненбаум Э.С., Уэзеролл Д. Компьютерные сети. 6-е изд. – СПб.: Питер, 2014. – 960 с.
7. Чердынцев Е.С. Мультимедийные сети: учеб. пособие/Е.С.Чердынцев - издательство Томского политехнического университета, 2014 – 96с.
8. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 6-е изд. – СПб.: Питер, 2014. – 944 с.
9. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА-М, 2011. – 192 с.
10. Поляк-Брагинский А.В. Администрирование сети на примерах. – СПб.: БХВ-

Петербург, 2005. – 320 с.
11. Хант К. TCP/IP. Сетевое администрирование. 3-е изд. – СПб.: Символ-плюс, 2008. – 816 с.
12. Чернега В., Платтнер Б. Компьютерные сети: Учебное пособие для вузов / В.Чернега, Б. Платтнер – Севастополь: Изд-во СевНТУ, 2006. – 500 с.

Интернет-ресурсы:

1. https://www.securitylab.ru/
2. https://xakep.ru/
3. https://securelist.ru/

9.3.Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsift Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Proffesional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 1000-1499 Node 2 year Educational Renewal License (лицензия 2022-190513-020932-503-526), срок пользования с 2019-05-13 по 2021-04-13
10. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
11. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
12. «Антиплагиат. ВУЗ». Лицензионный договор №194 от 22.03. 2018 года;

9.4.Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (https://habr.com/)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (https://github.com/)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (http://www.n-t.ru)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (http://znanium.com/)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (https://www.book.ru/)
8. Интернет-университет информационных технологий (www.intuit.ru)

9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)
11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
14. Polpred.com Обзор СМИ (http://polpred.com/)
15. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)
16. Электронная библиотечная система IPRbooks (http://www.iprbookshop.ru)
17. Электронная библиотечная система Национальная электронная библиотека (https://нэб.рф)
18. Электронная библиотечная система Юрайт (http://www.biblio-online.ru)

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю)*;*

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

(Изменения и дополнения в РПД вносятся ежегодно и оформляются в данной форме. Изменения вносятся заменой отдельных листов (старый лист при этом цветным маркером перечеркивается, а новый лист с изменением степлером прикалывается к рабочей программе (хранится на кафедре), в электронной форме РПД должна быть актуализированной всегда, т.е. с внесенными изменениями.

При наличии большого количества изменений и поправок, затрудняющих понимание, возникших в связи с изменением нормативной базы ВО и другим причинам, проводится полный пересмотр РПД (т.е. выпускается новая РПД), которая проходит все стадии проверки и утверждения).

в рабочей программе *(модуле)* дисциплины_____
(название дисциплины)
по направлению подготовки *(специальности)*_____

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата

Зав. кафедрой подпись расшифровка подписи