

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики
А.М. Райгородский**

	Рабочая программа дисциплины (модуля)
по дисциплине:	Современные компьютеры и сети передачи данных
по направлению:	Информатика и вычислительная техника
профиль подготовки:	Прикладная математика и информатика Физтех-школа Прикладной Математики и Информатики кафедра системного программирования
курс:	1
квалификация:	магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Дифференцированный зачет

Аудиторных часов: 30 всего, в том числе:

лекции: 15 час.

семинары: 15 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 15 час.

Всего часов: 45, всего зач. ед.: 1

Программу составил: В.З. Шнитман, д-р техн. наук, старший научный сотрудник

Программа обсуждена на заседании кафедры системного программирования 06.05.2024

Аннотация

Дисциплина "Современные компьютеры и сети передачи данных" изучает предмет, цели, задачи, структуру, основные понятия и общие сведения о сетях, основы построения сетей, архитектура и стандартизация сетей, требования к современным компьютерным сетям. Изучаются основы передачи дискретных данных: линии связи, методы кодирования и передачи дискретных данных на физическом уровне, методы передачи данных канального уровня, мультиплексирование и коммутация, беспроводная передача информации, первичные сети.

1. Цели и задачи

Цель дисциплины

- ознакомление студентов с современным состоянием и тенденциями стандартизации сетевых протоколов, в особенности в части вопросов обеспечения безопасности передачи информации.

Задачи дисциплины

- освоение студентами базовых знаний в области обеспечения безопасности передачи информации в компьютерных сетях;
- приобретение знаний о сервисах и механизмах безопасности, используемых в современных компьютерных сетях;
- оказание консультаций и помощи студентам в проведении собственных исследований и разработок в областях, использующих средства обеспечения безопасности, в частности для создания распределенных систем обработки информации;
- приобретение навыков работы в современных сетях компьютеров с использованием различных технологий обеспечения безопасности.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
	УК-1.3 Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности
ПК-3 Владеет навыками участия в научных дискуссиях, выступления с сообщениями и докладами устного, письменного и виртуального (размещение в информационных сетях) характера, представления материалов собственных исследований	ПК-3.1 Знает основы ведения научной дискуссии и формы устного научного высказывания
	ПК-3.2 Умеет вести корректную дискуссию в области информационных технологий задавать вопросы и отвечать на поставленные вопросы по теме научной работы
	ПК-3.3 Имеет практический опыт участия в научных студенческих конференциях, очных, виртуальных, заочных обсуждениях научных проблем в области информационных технологий
ПК-1 Готов к включению в профессиональное сообщество; способен	ПК-1.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации; владеет навыками подготовки научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке

проводить под научным руководством локальные исследования на основе существующих методов в конкретной области профессиональной деятельности

ПК-1.2 Умеет решать научные задачи с пониманием существующих подходов к верификации моделей программного обеспечения в связи с поставленной целью и в соответствии с выбранной методикой

ПК-1.3 Имеет практический опыт выступлений и научной аргументации при анализе объекта научной и профессиональной деятельности

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- стандартные методы организации открытых компьютерных сетей;
- основные угрозы нарушения безопасности в открытых компьютерных сетях;
- методы и средства противодействия угрозам нарушения безопасности в открытых компьютерных сетях, включая Интернет;
- стандартизованные методы криптографии, используемые для защиты информации в современных компьютерных сетях;
- методы аутентификации пользователей и других сущностей в компьютерных сетях;
- цели и методы обеспечения конфиденциальности и целостности данных;
- механизмы авторизации и контроля доступа к сетевым ресурсам;
- размещение сервисов безопасности в многоуровневой сетевой архитектуре и стандартизованные средства их реализации.

уметь:

- грамотно подобрать средства безопасности, необходимые при выполнении научных исследований с использованием компьютерных сетей;
- проводить самостоятельные научные исследования по теме дисциплины;
- применять изученные методы, протоколы и алгоритмы для решения поставленных задач.

владеть:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в Интернете;
- культурой обеспечения безопасности разработки и реализации системного программного обеспечения современных компьютеров и сетей.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Аутентификация. Контроль доступа.	2	2		
2	Безопасность электронной почты и электронного обмена документами. Управление сетью.	2	2		2
3	Инфраструктура открытых ключей (PKI). Справочные системы.	3	3		3
4	Конфиденциальность и целостность. Неотказуемость.	2	2		3
5	Обеспечение безопасности на транспортном уровне. Обеспечение безопасности на сетевом уровне.	2	2		2
6	Сервисы безопасности и уровневая архитектура. Методы криптографии.	3	2		3

7	Стандарты открытых систем. Концепции и терминология открытых систем. Основы безопасности сетей.	1	2		2
Итого часов		15	15		15
Подготовка к экзамену		0 час.			
Общая трудоёмкость		45 час., 1 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 1 (Осенний)

1. Аутентификация. Контроль доступа.

Общие концепции. Парольные механизмы. Противодействие внешнему разглашению и угадыванию пароля. Противодействие прослушиванию линии связи. Противодействие компрометации верификатора. Противодействие повторному воспроизведению. Другие механизмы, не использующие криптографию. Одноразовые пароли. Окрик-отзыв. Механизмы на основе адреса. Механизмы, использующие характерные особенности человека. Карты аутентификации личности. Использование методов криптографии. Роль оперативных серверов. Роль автономных серверов. Методы доказательства с нулевым разглашением. Аутентификация личности. Некоторые тонкости протоколов аутентификации. Атаки перехвата и повторного воспроизведения. Использование неповторяющихся значений. Протоколы взаимной аутентификации. Защита аутентификации.

Некоторые конкретные механизмы. Система Kerberos. Аутентификационные обмены X.509. Аутентифицированный обмен Диффи-Хеллмана. Стойкие парольные протоколы. Основная идея. Расширенная версия протокола ЕКЕ. Стойкий парольный протокол SRP. Аутентификация источника данных. Требования к протоколам. Аутентификационные обмены. Обмен информацией с оперативным сервером. Обмен информацией о сертификатах. Местоположение в архитектуре. Аутентификация сущностей. Аутентификация источника данных.

Политики контроля доступа. Механизмы контроля доступа. Списки контроля доступа. Возможности. Метки безопасности. Информационная модель, связанная с механизмами контроля доступа. Механизмы на основе паролей. Пример механизма контроля доступа из приложения FTAM. Общая модель распределения функций контроля доступа в сетевой среде. Требования к управлению и распространению информации, связанной с контролем доступа, в сетевой среде. Контроль доступа к коммуникациям и контроль маршрутизации. Требования к протоколам и вопросы определения местоположения в уровневой архитектуре.

2. Безопасность электронной почты и электронного обмена документами. Управление сетью.

Система обработки сообщений X.400 MHS (Общая архитектура. Администрирование систем обработки сообщений. Имена и адреса в MHS). Угрозы в среде MHS и сервисы безопасности, используемые для противодействия этим угрозам. Протокольные элементы MHS, используемые для обеспечения безопасности. Обеспечение основных сквозных сервисов безопасности MHS. Обеспечение других сервисов безопасности MHS. Методы безопасности, используемые в MHS. Специальные меры для защиты обмена транзакциями EDI.

Почта Интернет (Общая архитектура. Почтовые адреса. Списки рассылки. Многоцелевое расширение почты Интернет – MIME). Почта Интернет с расширениями конфиденциальности (PEM). Структура сообщения PEM. Установление ключей. Иерархия сертификатов PEM. Списки аннулированных сертификатов. Шифрование. Аутентификация источника и защита целостности. Сообщение для нескольких получателей. Пересылка сообщения и вложения. Незащищенная информация. Форматы сообщений.

Расширение почты Интернет – SMIME. Отличия S/MIME и PEM. Иерархия сертификатов S/MIME.

Почтовый протокол PGP. Обзор. Распределение ключей. Эффективное кодирование. Аннулирование сертификатов и ключей. Типы подписей. Закрытый ключ. Связка ключей. Форматы объектов.

Подход Интернет (Общая организация управления в Интернет. База управляющей информации. Структура управляющей информации. Протокол SNMP, SNMP и стек протоколов. Протоколы безопасности для SNMPv2). Управление сетями OSI (Модель управляющей информации OSI и GDMO. CMIP/CMIS, CMIP и семейство протоколов. CMIP и удаленные операции. Функции управления системой. Профили). Обеспечение безопасности управления сетью.

3. Инфраструктура открытых ключей (PKI). Справочные системы.

Модели доверия PKI. Модель монополии. Монополия плюс центры регистрации. Уполномоченные центры сертификации. Олигархия. Модель анархии. Ограничения имен. Модель «сверху-вниз» с ограничениями имен. Модель «снизу-вверх» с ограничениями имен. Относительные имена. Ограничения имен в сертификатах. Политики в сертификатах. Аннулирование сертификатов. PKI и справочные системы. Сертификаты PKIX и X.509. Авторизация с помощью PKI.

Модель телефонного справочника. Принципы организации справочной системы. Справочные службы открытых систем. Справочная система X.500. (Серия стандартов. Архитектура. Информационная модель справочной системы). Модель Справочной Системы (Службы справочной системы. Взаимодействие между агентами справочной службы. Протоколы справочной системы. Модель безопасности справочной системы). Система аутентификации X.509 (аутентификационные обмены, форматы сертификатов, процедуры управления сертификатами). Контроль доступа к справочной системе.

Упрощенный протокол доступа к справочной системе (LDAP).

Система доменных имен (Доменные имена. Как работает DNS. Обратный поиск. Обмен почтой). Расширения DNSSEC. Базовые принципы работы. Процедуры поиска. Доверенные анкеры и аутентификационные цепочки. Управление ключами.

4. Конфиденциальность и целостность. Неотказуемость.

Общие средства обеспечения конфиденциальности. Два подхода к обеспечению конфиденциальности. Средства управления потоками данных. Степень детализации данных. Конкретные типы механизмов конфиденциальности. Шифрование. Дополнение данных. Дополнение трафика. Другие механизмы. Общие средства обеспечения целостности. Уровень детализации данных. Восстановление. Конкретные типы механизмов целостности. Контрольные слова. Печати или подписи. Шифрование. Целостность последовательности. Дублирование. Восстановление целостности. Комбинирование механизмов конфиденциальности и целостности. Требования к протоколам, предъявляемые механизмами конфиденциальности и целостности. Криптографические преобразования. Управляющая информация протокола. Метки безопасности. Местоположение конфиденциальности и целостности в архитектуре системы. Дополнительные возможности физического оборудования.

Фазы и роли в процессе обеспечения неотказуемости. Запрос сервиса. Генерация свидетельства. Передача и сохранение свидетельства. Верификация свидетельства. Разрешение спора. Неотказуемость инициатора. Цифровая подпись инициатора. Цифровая подпись данных доверенной третьей стороной. Цифровая подпись доверенной третьей стороной дайджеста элемента данных. Маркер доверенной третьей стороны. Участие доверенной третьей стороны в процессе передачи данных. Комбинации механизмов. Использование меток времени. Неотказуемость от доставки. Подтверждение, подписанное получателем. Подтверждение получения маркером. Доверенный агент доставки. Двухэтапная доставка. Последовательные отчеты о доставке. Функции доверенных третьих сторон. Требования к протоколам.

5. Обеспечение безопасности на транспортном уровне. Обеспечение безопасности на сетевом уровне.

Семейство протоколов SSL/TLS. Краткая история. Базовый протокол SSL/TLS. Возобновление сеанса. Вычисление ключей. Аутентификация клиента. PKI, применяемая SSL. Согласование наборов шифров. Возможные виды атак на SSL/TLS. Форматы сообщений SSL/TLS.

Недостатки протокола IPv4. Краткий обзор протокола IPv6. Экранирование. Туннелирование. Обзор IPsec. Контексты безопасности. База данных контекстов безопасности. База данных политик безопасности. Типовое применение IPsec. Протоколы AH и ESP. Туннельный и транспортный режимы. Протоколы автоматического установления контекстов безопасности и управления ключами в Интернет. Обзор протокола IKE. Особенности работы протокола IKE. Структура сообщений ISAKMP/IKE.

6. Сервисы безопасности и уровневая архитектура. Методы криптографии.

Размещение сервисов безопасности в многоуровневой сетевой архитектуре. Безопасность прикладного уровня. Безопасность уровня оконечных систем. Безопасность уровня подсети. Безопасность уровня канала связи. Взаимодействие с людьми. Управление сервисами безопасности.

Симметричные криптосистемы. Типы алгоритмов и режимы шифрования. Режим электронной кодовой книги. Режим сцепления блоков шифра. Режим обратной связи по выходу. Режим обратной связи по шифру. Режим счетчика. Общие принципы построения блочных шифров. Стандарт шифрования данных DES. Усовершенствованный стандарт шифрования AES. Алгоритм ГОСТ 28147-89. Криптосистемы с открытым ключом. Алгоритм RSA. Алгоритм Эль Гамала. Коды аутентификации сообщений.

Цифровые подписи. Стандарт цифровой подписи США. Алгоритм цифровой подписи ГОСТ. Хэш-функции. Общие принципы управления криптографическими ключами. Методы распределения секретных ключей. Распределение ключей с помощью симметричных методов. Распределение ключей посредством принудительного обращения к серверу ключей. Распределение ключей с помощью методов реверсивных открытых ключей. Алгоритм создания ключа Диффи-Хеллмана. Методы распределения ключей для асимметричных криптосистем. Распределение открытых ключей. Генерация пары ключей. Аннулирование сертификатов. Пример: Инфраструктура сертификации PEM.

7. Стандарты открытых систем. Концепции и терминология открытых систем. Основы безопасности сетей.

Процессы стандартизации OSI и Internet. Стандарты, профили, соглашения по реализации и тестирование на соответствие стандартам.

Архитектуры. Открытые системы. Уровни. Краткий обзор семи уровней модели OSI. Краткий обзор уровней Internet. Терминология. Объекты. Система обозначений. Службы. Модель очередей. Службы с установлением и без установления соединения. Отношения между службами и протоколами. Протокольные заголовки и пользовательские данные. Временные диаграммы. Обзор служб распределенных приложений.

Политика безопасности. Угрозы и меры безопасности. Пять основных сервисов безопасности: аутентификация, контроль доступа, конфиденциальность, целостность данных и невозможность отказа. Обнаружение вторжений и аудит безопасности.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Необходимое оборудование для лекций: компьютер и мультимедийное оборудование (проектор, звуковая система).

6. Перечень рекомендуемой литературы

Основная литература

1. Танненбаум Э. Компьютерные сети. - СПб.: Питер, 2003.
2. Халсалл Ф. Передача данных, сети компьютеров и взаимосвязь открытых систем. - М.: Радио и связь, 1995.
3. Семенов Ю.А. Протоколы и ресурсы Internet. - М.: Радио и связь, 1996.
4. С. Бенет, С. Пэйн. Криптография. Официальное руководство RSA Security. - М.: Бином-Пресс, 2002.

Дополнительная литература

1. Б. Шнайер. Прикладная криптография. - М.: ТРИУМФ, 2003
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. - СПб.: БХВ-Петербург, 2009.
3. В.А. Галатенко. Основы информационной безопасности. - М.: ИНТУИТ.РУ «Интернет-Университет», 2003.
4. В.А. Галатенко. Стандарты информационной безопасности. - М.: ИНТУИТ.РУ «Интернет-Университет», 2004.
5. М.Р. Биктимиров, А.Ю. Щербаков. Избранные главы компьютерной безопасности. - Казань: Издательство Казанского математического общества, 2004.
6. К.В. Ребриков, В.З. Шнитман. "Протоколы автоматического установления контекстов безопасности и управления ключами в Интернет", Препринт 19 ИСП РАН, М., 2007.

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

<http://www.iso.org>, <http://www.itu.int>, <http://www.ietf.org>

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Программное обеспечение и информационные технологии не требуются.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике. В результате изучения дисциплины студент должен знать основные определения, понятия, аксиомы, методы доказательств.

Успешное освоение курса требует напряжённой самостоятельной работы студента. В программе курса приведено минимально необходимое время для работы студента над темой. Самостоятельная работа включает в себя:

- чтение и конспектирование рекомендованной литературы;
- проработку учебного материала (по учебной и научной литературе), подготовку ответов на вопросы, предназначенных для самостоятельного изучения, доказательство отдельных утверждений, свойств;
- выполнение лабораторных работ, для осознания связей между теорией и практическими навыками;
- подготовку к дифференцированному зачету.

Руководство и контроль за самостоятельной работой студента осуществляется в форме индивидуальных консультаций.

Важно добиться понимания изучаемого материала, а не механического его запоминания. При затруднении изучения отдельных тем, вопросов, следует обращаться за консультациями к лектору.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению: Информатика и вычислительная техника
профиль подготовки: Прикладная математика и информатика
Физтех-школа Прикладной Математики и Информатики
кафедра системного программирования
курс: 1
квалификация: магистр

Семестр, формы промежуточной аттестации: 1 (осенний) - Дифференцированный зачет

Разработчик: В.З. Шнитман, д-р техн. наук, старший научный сотрудник

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации
	УК-1.3 Разрабатывает стратегию достижения поставленной цели как последовательность шагов, предвидя результат каждого из них и оценивая их влияние на внешнее окружение планируемой деятельности и на взаимоотношения участников этой деятельности
ПК-3 Владеет навыками участия в научных дискуссиях, выступления с сообщениями и докладами устного, письменного и виртуального (размещение в информационных сетях) характера, представления материалов собственных исследований	ПК-3.1 Знает основы ведения научной дискуссии и формы устного научного высказывания
	ПК-3.2 Умеет вести корректную дискуссию в области информационных технологий задавать вопросы и отвечать на поставленные вопросы по теме научной работы
	ПК-3.3 Имеет практический опыт участия в научных студенческих конференциях, очных, виртуальных, заочных обсуждениях научных проблем в области информационных технологий
ПК-1 Готов к включению в профессиональное сообщество; способен проводить под научным руководством локальные исследования на основе существующих методов в конкретной области профессиональной деятельности	ПК-1.1 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации; владеет навыками подготовки научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и английском языке
	ПК-1.2 Умеет решать научные задачи с пониманием существующих подходов к верификации моделей программного обеспечения в связи с поставленной целью и в соответствии с выбранной методикой
	ПК-1.3 Имеет практический опыт выступлений и научной аргументации при анализе объекта научной и профессиональной деятельности

2. Показатели оценивания компетенций

В результате изучения дисциплины «Современные компьютеры и сети передачи данных» обучающийся должен:

знать:

- стандартные методы организации открытых компьютерных сетей;
- основные угрозы нарушения безопасности в открытых компьютерных сетях;
- методы и средства противодействия угрозам нарушения безопасности в открытых компьютерных сетях, включая Интернет;
- стандартизованные методы криптографии, используемые для защиты информации в современных компьютерных сетях;
- методы аутентификации пользователей и других сущностей в компьютерных сетях;
- цели и методы обеспечения конфиденциальности и целостности данных;
- механизмы авторизации и контроля доступа к сетевым ресурсам;
- размещение сервисов безопасности в многоуровневой сетевой архитектуре и стандартизованные средства их реализации.

уметь:

- грамотно подобрать средства безопасности, необходимые при выполнении научных исследований с использованием компьютерных сетей;
- проводить самостоятельные научные исследования по теме дисциплины;
- применять изученные методы, протоколы и алгоритмы для решения поставленных задач.

владеть:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в Интернете;
- культурой обеспечения безопасности разработки и реализации системного программного обеспечения современных компьютеров и сетей.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

С целью контроля освоения обучающимися учебного материала проводится устный опрос в начале занятия по теме прошлой лекции или в конце занятия по пройденной теме.

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

1. Зачем нужны стандарты, профили, соглашения по реализации и тестирование на соответствие стандартам?
2. Поясните отношения между сетевыми службами и протоколами.
3. Семиуровневая модель взаимосвязи открытых систем OSI.
4. Стек протоколов TCP/IP.
5. Классификация угроз и мер безопасности.
6. Сервисы безопасности.
7. Размещение сервисов безопасности в многоуровневой архитектуре.
8. Симметричные криптосистемы. Приведите примеры стандартных алгоритмов.
9. Асимметричные криптосистемы. Приведите примеры стандартных алгоритмов.
10. Коды MAC.
11. Цифровые подписи.
12. Распределение секретных ключей.
13. Распределение ключей криптосистем с открытым ключом.
14. Общие концепции аутентификации.
15. Парольные системы.
16. Система Kerberos.
17. Аутентификационные обмены X.509.
18. Аутентифицированный обмен Диффи-Хеллмана.
19. Основная идея и реализации стойких парольных протоколов.
20. Политики и механизмы контроля доступа.
21. Общие средства обеспечения конфиденциальности и конкретные типы механизмов конфиденциальности.
22. Общие средства обеспечения целостности.
23. Фазы и роли в процессе обеспечения неотказуемости. Механизмы неотказуемости.
24. Инфраструктуры открытых ключей и модели доверия PKI.
25. Язык ASN.1
26. Справочная система X.500. Модель безопасности справочной системы.
27. Упрощенный протокол доступа к справочной системе (LDAP).
28. Система доменных имен. Расширения DNSSEC.
29. Система обработки сообщений MHS X.400. Угрозы в среде MHS и сервисы безопасности, используемые для противодействия этим угрозам.
30. Почта Интернет. Расширение почты Интернет – SMIME. Отличия S/MIME, PEM и PGP.
31. Протокол SNMP и организация управления в Интернет. Обеспечение безопасности управления сетью.
32. Транспортный уровень в семействе TCP/IP. Семейство протоколов SSL/TLS.
33. Межсетевой уровень в семействе TCP/IP. Недостатки IPv4 и возможности IPv6.
34. Механизмы экранирования и туннелирования в Интернет.

- 35. Типовое применение IPsec.
- 36. Протоколы AH и ESP.
- 37. Туннельный и транспортный режимы.
- 38. Основной и агрессивный режимы IKE.
- 39. Быстрый режим IKE.

Критерии оценивания

Оценка отлично 10 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 9 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.

Оценка отлично 8 баллов - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.

Оценка хорошо 7 баллов - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.

Оценка хорошо 6 баллов - выставляется студенту, если он 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 хорошо 5 баллов - выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.

Оценка удовлетворительно 4 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.

Оценка удовлетворительно 3 балла - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет полученные знания даже в стандартной ситуации.

Оценка неудовлетворительно 2 балла - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.

Оценка неудовлетворительно 1 балл - выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Во время проведения дифференциального зачёта обучающиеся могут пользоваться программой дисциплины, а также справочной литературой, вычислительной техникой, конспектами лекций. Дифференциальный зачёт проводится путем организации специального опроса, проводимого в устной форме.