МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Санкт-Петербургский государственный технологический институт (технический университет)»

УТВЕРЖДАЮ
Проректор по учебной
и методической работе
_____ Б.В.Пекаревский
«_____» _____ 2016 г.

Рабочая программа дисциплины
Интернет-технологии

Направленность программы бакалавриата
09.03.01 Информатика и вычислительная техника

Направленности программы бакалавриата
Автоматизированные системы обработки информации и управления

Квалификация
Бакалавр

Форма обучения
Заочная

Факультет **информационных технологий и управления**
Кафедра **систем автоматизированного проектирования и управления**

Санкт-Петербург
2016

ЛИСТ СОГЛАСОВАНИЯ

Должность	Подпись	Ученое звание, фамилия, инициалы
Разработчики		Новикова О.Г.

Рабочая программа дисциплины «Интернет-технологии» обсуждена на заседании кафедры систем автоматизированного проектирования и управления
протокол от «13» апреля 2016 № 7
Заведующий кафедрой Т.Б. Чистякова

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от «15» апреля 2016 № 7

Председатель В.В.Куркина

СОГЛАСОВАНО

Руководитель направления подготовки «Информатика и вычислительная техника»		профессор Т.Б. Чистякова
Директор библиотеки		Т.Н.Старостенко
Начальник методического отдела учебно-методического управления		Т.И.Богданова
Начальник УМУ		С.Н.Денисенко

СОДЕРЖАНИЕ

Приложения: 1. Фонд оценочных средств для проведения промежуточной аттестации.

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

В результате освоения образовательной программы бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ООП *(содержание компетенций)*	Перечень планируемых результатов обучения по дисциплине
ПК-1	способность разрабатывать модели компонентов информационных систем, включая модели баз данных и модели интерфейсов "человек – электронно-вычислительная машина";	**Знать:** Принципы и технологии глобальных сетей и сетей доступа Сетевые операционные системы Основные определения, классификацию и эксплуатационные характеристики локальных информационных сетей **Уметь:** Анализировать структуру корпоративной сети Обосновать применение протоколов маршрутизации Использовать прикладные протоколы и сервисы Использовать стандартные протоколы стека TCP/IP для организации сетевого для организации взаимодействия приложений в распределенной системе Выполнять инсталляцию и первоначальную настройку сетевой ОС **Владеть:** Навыками конфигурирования сетевого оборудования и программного обеспечения Навыками использования современных программных средств
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** типы подключения к глобальной сети; способы создания виртуально-независимого канала в глобальной сети (VPN); протоколы стека TCP/IP; Протоколы защищенной передачи данных IPSec, SSL/TLS **Уметь:** использовать системные и прикладные программы для

Коды компетенции	Результаты освоения ООП *(содержание компетенций)*	Перечень планируемых результатов обучения по дисциплине
		обеспечения безопасного и отказоустойчивого соединения с глобальной сетью Internet; **Владеть:** навыками проектирования корпоративных сетей.
ПК-2	способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования	**Знать:** компоненты информационных сетей (коммуникационные подсети моноканальные подсети, циклические подсети, узловые подсети) методы коммутации информации; непрерывный и дискретный каналы связи протоколы маршрутизации в IP-сетях и их характеристики; методы защиты от ошибок и обеспечения безопасности информации; **Уметь:** выбирать компоненты сетевого оборудования информационной сети и оценивать их характеристики; использовать методы и средства информационных сетей при создании комплексов обработки информации **Владеть:** методами проектирования защищенных корпоративных сетей и оценки их характеристик

2. Место дисциплины в структуре образовательной программы.

Дисциплина относится к обязательным дисциплинам вариативной части (Б1.В.ОД.1) и изучается на 4 курсе в 7 и 8 семестрах.

В методическом плане дисциплина опирается на элементы компетенций, сформированные при изучении дисциплин «Информатика», «Вычислительные системы, сети и телекоммуникации».

Полученные в процессе изучения дисциплины «Интернет-технологии» знания, умения и навыки могут быть использованы для подготовки и написания выпускной квалификационный работы бакалавра.

3. Объем дисциплины.

Вид учебной работы	Всего, академических часов
	Очная форма обучения
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	5/ 180
Контактная работа с преподавателем:	**16**
занятия лекционного типа	6
занятия семинарского типа, в т.ч.	10
семинары, практические занятия	4
лабораторные работы	6
курсовое проектирование (КР или КП)	КП
КСР	9
другие виды контактной работы	
Самостоятельная работа	**155**
Форма текущего контроля (Кр)	**Контрольные работы**
Форма промежуточной аттестации (КП , экзамен)	Курсовой проект, экзамен (36)

4. Содержание дисциплины.

4.1. Разделы дисциплины и виды занятий.

№ п/п	Наименование раздела дисциплины	Занятия лекционного типа, акад. часы	Занятия семинарского типа, академ. часы		Самостоятельная работа, акад. часы	Формируемые компетенции
			Семинары и/или практические занятия	Лабораторные работы		
1.	Аппаратное обеспечение и принципы функционирования корпоративных сетей	1		1	30	ПК-1, ОПК-5, ПК-2
2.	Прикладные сервисы Intranet	1		1	30	ПК-1, ПК-2
3.	Алгоритмы маршрутизации	1		1	30	ПК-2
4.	Основы построения защищенных информационных систем	1		1	30	ОПК-5, ПК-2

5.	Проектирование систем информационной безопасности корпоративных сетей	2	4	2	35	ОПК-5

4.2. Занятия лекционного типа.

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	**Аппаратное обеспечение и принципы функционирования корпоративных сетей** Структура глобальной сети. Перспективы развития, основные направления новых исследований. Функции федеральных, региональных и местных узлов. Определение провайдера. Необходимое оборудование. Виды услуг и сервисов провайдера.	1	
2	**Прикладные сервисы Intranet.** Протокол RARP, как предшественник протокола DHCP. Протокол DHCP.Система DNS. Первичный и вторичный сервера DNS. Реверсные запросы. **Сервис электронной почты.** Пользовательский клиент – функции, алгоритм работы. Транспортный агент. Доставочный агент.	1	
3	**Алгоритмы маршрутизации** Протокол OSPF. Многокритериальность: надёжность, скорость, цена, уплотнение. Алгоритм Дейкстры. Таблицы маршрутизации. Маршрутизатор-мастер. Протокол RIP. Критерий маршрутизации. Формат кадра. Алгоритм работы.	1	
4	**Основы построения защищенных информационных систем** VPN**.** Принципы создания виртуально независимого канала интернет. Криптошлюз. Организация доступа через сервер безопасности. Демилитаризованная зона.	1	
5	**Проектирование систем информационной безопасности корпоративных сетей** Firewall – функции, виды, способы размещения. Шифрование на аппаратном уровне – криптоплаты. Шифрование через туннель. Шифрование на уровне данных.Угрозы социальных сетей. Чёрный рекламщик. Аутсорсинг. HoneyPot – типы, способы размещения. IDS/IPS –особенности работы	2	

4.3. Занятия семинарского типа.

4.3.1. Семинары, практические занятия.

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
5	**Проектирование систем информационной безопасности корпоративных сетей** Firewall – функции, виды, способы размещения.	1	Интерактивные тренинги по выбору типа и конфигурации Firewall

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
5	**Проектирование систем информационной безопасности корпоративных сетей** Шифрование на аппаратном уровне – криптоплаты. Шифрование через туннель. Шифрование на уровне данных	1	Доклады, основанные на методике создания «кейсов»
5	**Проектирование систем информационной безопасности корпоративных сетей** Аутсорсинг. HoneyPot –типы, способы размещения.	1	Применение методики развития критического мышления -ТРКМ
5	**Проектирование систем информационной безопасности корпоративных сетей** IDS/IPS –особенности работы	1	Обсуждения индивидуально-ориентированных маршрутов, в контексте бакалаврской работы

4.3.2. Лабораторные занятия.

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Примечание
1	Аппаратное обеспечение и принципы функционирования корпоративных сетей	1	Контрольная работа
2	Прикладные сервисы Intranet. Использование Web-технологий для создания Интернет-порталов.	1	Защита программного продукта
4	Основы построения защищенных информационных систем	1	
5	Проектирование систем информационной безопасности корпоративных сетей	1	
3	Алгоритмы маршрутизации	2	Контрольная работа

4.4. Самостоятельная работа обучающихся.

№ раздела дисциплины	Перечень вопросов для самостоятельного изучения	Объем, акад. часы	Форма контроля
1	Аппаратное обеспечение и принципы функционирования корпоративных сетей. Стандарты и	30	Контрольная работа

	методы построения цифровых каналов.		
2	Прикладные сервисы Intranet. Многоуровневые гетерогенные интерфейсы для организации обработки запроса клиента по протоколу http.	30	Письменный опрос
3	Алгоритмы маршрутизации. Особенности построения Российского сегмента.	30	Устный опрос
4	Основы построения защищенных информационных систем. Аутентификация по биометрическим характеристикам.	30	Устный опрос
5	Проектирование систем информационной безопасности корпоративных сетей. Определение ущерба для корпорации, исходя из состава атакуемых данных.	35	Контрольная работа

4.4.1. Темы контрольных работ

Предлагаемые ниже вопросы могут быть использованы для промежуточной аттестации и контроля над уровнем усвоения учебного материала студентами. Предполагается написание студентами письменных контрольных работ, в которые включен один из предложенных вариантов списка. Число таких проверочных работ в течение семестра – 3. Контрольные работы проводятся, как правило, после изучения очередной темы

ВАРИАНТ 1

1. Что такое депозитарий;
2. Что такое соединители;
3. В чем заключается процедура handshake;
4. Формат кадра UDP;
5. 4 функции сетевых операционных систем;
6. 2 вида деления одноранговых сетей по функциональному признаку;
7. Перечислить ограничения, которые могут налагаться при проектировании информационной безопасности средствами сетевых операционных систем;
8. Механизм электронной подписи
9. Сущность защиты информации на сетевом уровне;
10. Реализация отказоустойчивости стандартными способами;
11. 4 вида RAID, их отличия;
12. Запросы и отклики управляющего протокола SNMP;
13. Программная оболочка рабочей станции в Novell NetWare;
14. Право Access Control в системе защиты через права Novell NetWare;
15. Система трассировки транзакций в Novell NetWare;
16. Что такое модуляция;
17. Спутниковые модемы;
18. 3 способа подключения к провайдеру.

ВАРИАНТ 2

1. В каких задачах требования к протоколам увеличиваются;
2. Функции соединителя в TCP;
3. Состояние компьютера passive open и active open в TCP;

4. Принципы работы протокола UDP;
5. Реализация файловой подсистемы в сетевых операционных системах в одноранговых сетях;
6. Информационная безопасность. Функции специального ПО;
7. Разграничение доступа при помощи специального ПО;
8. Требования, предъявляемые к информационной безопасности системы по стандарту С2;
9. Схема кластеризации серверных систем пассивный/активный;
10. В чем особенность управляющего протокола SNMP;
11. Особенности загрузки исполняемых файлов *.nlm в сетевой операционной системе Novell NetWare;
12. Программная оболочка рабочей станции в Novell NetWare;
13. Как реализована система защиты в Novell NetWare;
14. Система трассировки транзакций в Novell NetWare;
15. Типы модемов;
16. Структура сегмента RUNNET;
17. DNS – сервер;
18. Виртуальная реальность в Internet.

ВАРИАНТ 3

1. Что такое программа – демон;
2. Проиллюстрировать процесс передачи данных по TCP кадрами;
3. Таймеры TCP;
4. Принципы работы протокола UDP;
5. Деление серверов по функциональному признаку;
6. Симметричная и асимметричная обработка данных в серверах приложений;
7. Информационная безопасность. Как реализуется аутентификация при использовании специального ПО;
8. Что такое уровень готовности;
9. Реализация функции управления сетью в одноранговых сетях
10. Управление сетью. Структура Management Information Base.
11. Программная оболочка рабочей станции в Novell NetWare;
12. Право Modify в системе защиты через права Novell NetWare;
13. Система трассировки транзакций в Novell NetWare;
14. Средства связи в Internet;
15. Кабельные модемы;
16. Структура Uniform Resource Locator;
17. Схемы соединения узлов WWW;
18. Виртуальная реальность в Internet.

ВАРИАНТ 4

1. Как обеспечивается обработка нескольких запросов протоколом TCP;
2. Отличия флагов PSH и URG в TCP;
3. Что содержится в поле “опции” в кадре TCP;
4. Чем характеризуется состояние half-close в TCP;
5. Формат кадра протокола UDP;
6. Как организуется дуплексное соединение в файловой подсистеме сетевых операционных систем одноранговых сетей;
7. 3 способа организации ПО сервера;
8. Информационная безопасность. Реализация ограничения на удаленный доступ.
9. Схема кластеризации серверных систем активный/активный;
10. Разграничение множественного доступа к RAID при помощи Distributed Lock Manager.
11. Протокол управления сетью SNMP. В каких случаях возникает отклик trip.

12. Программная оболочка рабочей станции в Novell NetWare;
13. Средства, реализованные в файловой подсистеме Novell NetWare.
14. Право Create в системе защиты через права Novell NetWare;
15. Атрибут Archive Needed в системе защиты через атрибуты Novell NetWare;
16. Проиллюстрировать различные виды модуляции;
17. Схема запроса в Internet;
18. Функции Proxy – сервера.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине.

Методические указания для обучающихся по организации самостоятельной работы по дисциплине, включая перечень тем самостоятельной работы, формы текущего контроля по дисциплине и требования к их выполнению размещены в электронной информационно-образовательной среде СПбГТИ(ТУ) на сайте: http://media.technolog.edu.ru

6. Фонд оценочных средств для проведения промежуточной аттестации

Своевременное выполнение обучающимся мероприятий текущего контроля позволяет превысить (достигнуть) пороговый уровень («удовлетворительно») освоения предусмотренных элементов компетенций.

Результаты дисциплины считаются достигнутыми, если для всех элементов компетенций превышен (достигнут) пороговый уровень освоения компетенции на данном этапе.

Промежуточная аттестация по дисциплине проводится в форме экзамена в 6 семестре и защиты курсового проекта в 7 семестре.

К сдаче экзамена допускаются студенты, выполнившие все формы текущего контроля.

Экзамен предусматривают выборочную проверку освоения предусмотренных элементов компетенций и комплектуются вопросами (заданиями).

При сдаче экзамена, студент получает три вопроса из перечня вопросов, время подготовки студента к устному ответу - до 30 мин.

Пример варианта вопросов на экзамене:

Вариант № 1

1. Принципы построения отказоустойчивых систем.
2. Парадигмы семейства протоколов TCP/IP.
3. Структура объединенной компьютерной сети образования, науки и культуры.

Фонд оценочных средств по дисциплине представлен в Приложении № 1

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

1. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации : учеб. пособие для вузов / В. Л. Бройдо, О. П. Ильина. – 4-е изд. – М. ; СПб. ; Н. Новгород : Питер, 2011. – 554 с.

2. Головин, Ю. А. Информационные сети : учеб. для вузов / Ю. А. Головин, А. А. Суконщиков, С. А. Яковлев. – М. : Академия, 2011. – 376 с.

3. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 5-е изд., стер. – М. : Академия, 2011. – 331 с.

4. Схиртладзе, А. Г. Информационные технологии : учебник для вузов / [А. Г. Схиртладзе и др.]. - М. : Академия, 2015. - 288 с.

5. Норенков, И. П. Автоматизированные информационные системы : учеб. пособие / И. П. Норенков. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2011. – 342 с.

6. Тенишев, Д. Ш. Лингвистическое и программное обеспечение автоматизированных систем : учеб. пособие для вузов / Д. Ш. Тенишев ; под ред. Т. Б. Чистяковой. – СПб. : ЦОП «Профессия», 2010. – 403 с.

7. Хорошевский, В. Г. Архитектура вычислительных систем : учеб. пособие для вузов / В. Г. Хорошевский. – 2-е изд. – М. : Изд-во МГТУ им. Н.Э.Баумана, 2008. – 520 с.

б) дополнительная литература:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учеб. пособие для вузов / А. А. Афанасьев [и др.] ; под ред. А. А. Шелупанова [и др.]. – М. : Горячая линия – Телеком, 2009. – 552 с.

2. Олифер, В. Г. Сетевые операционные системы / В. Г. Олифер, Н. А. Олифер. – М. ; СПб. ; Н. Новгород : Питер, 2008. – 668 с.

3. Петкович, Д. Microsoft SQL Server 2008. Руководство для начинающих / Д. Петкович ; пер. с англ. – СПб. : БХВ-Петербург, 2012. – 730 с.

4. Рассел, Ч. Microsoft Windows Server 2008. Справочник администратора / Ч. Рассел, Ш. Кроуфорд ; пер. с англ. – М. : ЭКОМ, 2009. – 1321 с.

5. Станек, У. Р. Microsoft Windows Server 2003. Справочник администратора / У. Р. Станек ; пер. с англ. – 2-е изд., доп. – М. : Русская редакция, 2009. – 628 с.

6. Станек, У. Р. Windows Server 2008. Справочник администратора / У. Р. Станек ; пер. с англ. – 2-е изд., доп. – М. : Русская редакция ; СПб. : БХВ-Петербург, 2009. – 668 с.

7. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособие для вузов / В. Ф. Шаньгин. – М. : ДМК-Пресс, 2008. – 542 с.

8. Информационные технологии : ежемес. теорет. и прикл. науч.-техн. журн. – М. : Новые технологии, 2008– .

9. Программные продукты и системы : ежекварт. прил. к междунар. журн. «Проблемы теории и практики управления». – Тверь : МНИИПУ : НИИ «Центрпрограммсистем», 2008– .

в) вспомогательная литература:

1. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для вузов / В. В. Платонов. – М. : Академия, 2006. – 239 с.

2. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для вузов / П. Б. Хорев. – М. : Академия, 2005. – 255 с.

3. Хорев, П. Б. Технологии объектно-ориентированного программирования / П. Б. Хорев. – М. : Академия, 2008. – 448 с.

4. Чекмарев, А. Н. Microsoft Windows 7 для пользователей / А. Н. Чекмарев. – СПб. : БХВ-Петербург, 2010. – 541 с.

5. Чекмарев, Ю. В. Вычислительные системы, сети и телекоммуникации / Ю. В. Чекмарев. – Изд. 2-е, испр. и доп. – М. : ДМК-Пресс, 2010. – 184 с.

6. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации : учеб. для вузов / В. Л. Бройдо, О. П. Ильина. – 4-е изд. – СПб. : Питер, 2011. – 560 с.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

учебный план, РПД и учебно-методические материалы: http://media.technolog.edu.ru

сайты фирм разработчиков АСУТП: www.adastra.ru; www.foit.ru; www.metso.ru; www.siemens.ru;

электронно-библиотечные системы:

«Электронный читальный зал – БиблиоТех» https://technolog.bibliotech.ru/;

«Лань» https://e.lanbook.com/books/.

9. Методические указания для обучающихся по освоению дисциплины.

Все виды занятий по дисциплине «Интернет-технологии» проводятся в соответствии с требованиями следующих СТП:

СТО СПбГТИ 020-2011. КС УКДВ. Виды учебных занятий. Лабораторные занятия. Общие требования к организации и проведению.

СТП СПбГТИ 040-02. КС УКДВ. Виды учебных занятий. Лекция. Общие требования;

СТО СПбГТИ 018-2014. КС УКДВ. Виды учебных занятий. Семинары и практические занятия. Общие требования к организации и проведению.

СТП СПбГТИ 048-2009. КС УКДВ. Виды учебных занятий. Самостоятельная планируемая работа студентов. Общие требования к организации и проведению.

Планирование времени, необходимого на изучение данной дисциплины, лучше всего осуществлять на весь семестр, предусматривая при этом регулярное повторение пройденного материала.

Основными условиями правильной организации учебного процесса для студентов является:

плановость в организации учебной работы;

серьезное отношение к изучению материала;

постоянный самоконтроль.

На занятия студент должен приходить, имея багаж знаний и вопросов по уже изученному материалу.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

10.1. Информационные технологии.

В учебном процессе по данной дисциплине предусмотрено использование информационных технологий:

чтение лекций с использованием слайд-презентаций;

взаимодействие с обучающимися посредством электронной почты.

10.2. Программное обеспечение.

В учебном процессе используется лицензионное системное и прикладное программное обеспечение, приведенное в таблице 1.

Таблица 1 – Лицензионное программное обеспечение

Наименование программного продукта	Лицензия
Microsoft Windows XP, 7, 8.1	Лицензия по договору с СПбГТИ(ТУ) DreamSpark
Microsoft Visual Studio 2008, 2010, 2012	
Microsoft Visual C++ 2008	
Microsoft Microsoft .Net Framework 4.0, 4.5	
Microsoft Access 2007, 2013	

Наименование программного продукта	Лицензия
Microsoft Visio 2010	
LibreOffice, Apache OpenOffice.org	Бесплатная лицензия
ОС FreeBSD	Бесплатная лицензия

10.3. Информационные справочные системы.

Справочно-поисковая система «Консультант-Плюс»

11. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Для проведения занятий по дисциплине на кафедре систем автоматизированного проектирования и управления СПбГТИ(ТУ) имеется необходимая материально-техническая база, соответствующая действующим санитарным и противопожарным правилам и нормам:

Наименование компьютерного класса кафедры	Оборудование
Класс интегрированных систем проектирования и управления химико-технологическими процессами	30 посадочных мест. Учебная мебель, пластиковая доска. Персональные компьютеры (15 шт.): двухядерный процессор Intel Core 2 Duo (2,33 ГГц); ОЗУ 4096 Мб; НЖМД 250 Гб; CD/DVD привод, DVD-RW; видеокарта NVIDIA GeForce 8500 GT; звуковая и сетевая карты, встроенные в материнскую плату. Персональные компьютеры объединены в корпоративную вычислительную сеть кафедры и имеют выход в сеть «Интернет».
Класс информационных и интеллектуальных систем	40 посадочных мест. Учебная мебель, пластиковая доска. Персональные компьютеры (20 шт.): четырехядерный процессор Intel Core i7-920 (2666 МГц), ОЗУ 6 Гб; НЖМД 250 Гб; CD/DVD привод, DVD-RW; видеокарта NVIDIA GeForce GT 220 (1024 Мб); звуковая и сетевая карты, встроенные в материнскую плату. Персональные компьютеры объединены в корпоративную вычислительную сеть кафедры и имеют выход в сеть «Интернет».
Лекционная аудитория	56 посадочных мест. Учебная мебель. Мультимедийный проектор NEC NP41. Ноутбук Asus a6j на базе процессора Intel Core Duo T2000. Мультимедийная интерактивная доска ScreenMedia.

Лицензионное системное и прикладное программное обеспечение, используемое в учебном процессе по дисциплине, перечислено в подразделе № 10.2.

12. Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья.

Для инвалидов и лиц с ограниченными возможностями учебные процесс осуществляется в соответствии с Положением об организации учебного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья СПбГТИ(ТУ), утвержденным ректором 28.08.2014г.

Приложение № 1
к рабочей программе дисциплины

Фонд оценочных средств
для проведения промежуточной аттестации по
дисциплине «Интернет-технологии»

1. Перечень компетенций и этапов их формирования.

Компетенции		
Индекс	**Формулировка**	**Этап формирования**
ПК-1	способностью к самоорганизации и самообразованию	промежуточный
ОПК-5	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	промежуточный
ПК-2	способностью эксплуатировать и сопровождать информационные системы и сервисы.	промежуточный

2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкала оценивания.

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компе-тенции
Освоение раздела **№ 1**	Знает компоненты информационных сетей; методы коммутации; непрерывный и дискретный каналы связи **Умеет** выбирать компоненты сетевого оборудования информационной сети и оценивать их характеристики;	Выполнение контрольной работы № 1	ПК-1

Показатели оценки результатов освоения дисциплины	Планируемые результаты	Критерий оценивания	Компе-тенции
	Знает протоколы маршрутизации в IP-сетях и их характеристики; методы защиты от ошибок и обеспечения безопасности информации;	Правильные ответы на вопросы №38-46	ПК-2
	Владеет методами проектирования защищенных корпоративных сетей и оценки их характеристик	Правильные ответы на вопросы №16-22	ОПК-5
Освоение раздела №2	**Знает** типы подключения к глобальной сети; способы создания виртуально-независимого канала в глобальной сети (VPN); **Умеет** использовать системные и прикладные программы для обеспечения безопасного и отказоустойчивого соединения с глобальной сетью Internet;	Правильные ответы на вопросы №23-30	ОПК-5
	Знает протоколы стека TCP/IP; протоколы защищенной передачи данных IPSec, SSL/TLS	Правильные ответы на вопросы №32-38	ПК-2
Освоение раздела № 3	**Знает** протоколы маршрутизации в IP-сетях и их характеристики;	Успешная защита отчета по лабораторной работе № 3	ПК-2
Освоение раздела №4	**Умеет** выбирать компоненты сетевого оборудования информационной сети и оценивать их характеристики; использовать методы и средства информационных сетей при создании комплексов обработки информации	Правильные ответы на вопросы №16-22	ОПК-5
	Знает методы защиты от ошибок и обеспечения безопасности информации;	Успешное выполнение контрольной работы	ПК-2
Освоение раздела № 5	**Владеет** методами проектирования защищенных корпоративных сетей и оценки их характеристик	Успешное выполнение и защита курсового проекта	ОПК-5

Шкала оценивания соответствует СТО СПбГТИ(ТУ):

промежуточная аттестация проводится в форме экзамена и защиты курсового проекта, результаты оценивания – «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

3. Типовые контрольные задания для проведения промежуточной аттестации.

а) Вопросы для оценки сформированности элементов компетенции ПК-1:

1. Принципы построения отказоустойчивых систем.
2. Парадигмы семейства протоколов TCP/IP.
3. Структура объединенной компьютерной сети образования, науки и культуры.
4. Аппаратное и программное обеспечение модемов.
5. ADSL-модемы.
6. Кабельные модемы.
7. Радио-модемы.
8. Основные задачи proxy- сервера.
9. Задачи сервиса разрешения имен.
10. Служба новостей USENet.
11. Удаленный терминал и терминальные серверы.
12. Сетевая файловая система.
13. DHCP- протокол.
14. Метод трансляции сетевого адреса.
15. Кадр протокола DNS.

б) Вопросы для оценки сформированности элементов компетенции ОПК-5:

16. Авторитетные сервера DNS.
17. Понятия домена и зоны.
18. Записи базы данных DNS.
19. Таймеры DNS.
20. Почтовые агенты.
21. Использование автономных систем в почтовых программах.
22. Унифицированный указатель ресурса.
23. Посредник-шлюз.
24. Посредник-тоннель.
25. Посредник-proxy.
26. Протокол маршрутизации RIP.
27. Протокол маршрутизации OSPF.
28. Протокол IP6. Адресация.
29. Протокол IP6. Формат кадра.
30. Особенности передачи мультимедийных структур по каналам региональных сетей.
31. Форматы MPEG, JPG.

в) Вопросы для оценки сформированности элементов компетенции ПК-2:

32. IP-телефония.
33. Принципы проектирования распределенных систем управления.
34. Алгоритм проектирования систем информационной безопасности.
35. Расчет рисков.
36. Категории защиты.
37. Appliance.
38. Коммутация сообщений.
39. Модуляция в электрических сетях связи.
40. Код Хэмминга для проверки корректности передачи.
41. Разделяемы виртуальные миры.
42. Технология глобальной сети X-25.
43. Системы на базе стандарта X-400.
44. Системы на основе частных стандартов.
45. Гибридные системы.
46. Почтовый каталог.

47. Службы совместного использования информации.
48. Оперативное управление ОС NetWare.

К экзамену допускаются студенты, выполнившие все формы текущего контроля. При сдаче экзамена, студент получает два вопроса из перечня, приведенного выше.

Время подготовки студента к устному ответу на вопросы - до 30 мин.

Темы и содержание курсового проекта

Примеры тем курсовых проектов

1. Проектирование системы информационной безопасности для организации документооборота на заводе по производству промышленных смазок «Русма»
2. Проектирование системы информационной безопасности корпоративной сети для интерактивного общения клиентов с офисом продаж завода «Призма»
3. Проектирование системы информационной безопасности корпоративной сети для внедрения системы автоматизированного управления на заводе по производству изделий из пластмассы различного профиля «Восток»

Курсовой проект предназначен для углубления знаний о принципах проектирования корпоративных сетей, характеризующихся большим количеством компьютеров; наличием тонких клиентов с доступом к серверам разного функционального назначения; сегменты таких сетей территориально независимы. Студенты готовят материал о различных аспектах объекта проектирования. Разрабатывают проект сети для выбранного объекта проектирования. Особое внимание уделяется принципам проектирования системы информационной безопасности, как основной составляющей таких сетей.

Содержание курсового проекта:

Для обеспечения информационной безопасности корпорации разработать 3 составляющие:

1. Защита от несанкционированного доступа.

В рамках этого этапа выполнить:

1.1 Регистрация: при доступе к серверу или использовании рабочих станций в качестве депозитария:

1.1.1 двусторонняя идентификация клиентов; при успешном прохождении - односторонняя идентификация пользователя.

1.1.2 На этапе аутентификации предложить механизм генерации одноразовых паролей с периодическим сканированием (при запросе доступа к ключевым источникам информации) биометрических характеристик (стандартные аппаратные средства сканирования.

1.1.3Авторизацию осуществить времянными рамками входа. При запросах к удаленному компьютеру, дополняется ограничением числа сеансов (1) одного и того же пользователя. При запросе доступа к ключевому источнику информации -ограничением времени использования.

1.2 Ограничения прав доступа к объектам корпоративной сети через права и атрибуты организовать средствами ОС UNIX (формирование модели доверия: обследование коллектива сотрудников с целью выявления возможных инсайдеров; разбиение всей информации по классам защиты, в зависимости от важности информации и последствий её утечки).

1.3 Защита ключевых источников информации. Предложить использование стандартных средств защиты: датчики движения с оповещением; защита от физического извлечения жесткого диска; шифрование информации «на лету». Создать кластер типа «активный/активный» с функциями балансировки нагрузки и высокой доступности.

Обеспечение отказоустойчивости заключается в использовании дублирующих линий связи и линий энергоснабжения. Для хранения данных предлагается использование SAN.
2. Защита от внутренних нарушений политики безопасности.
2.1 В состав корпорации входят мобильные информационные объекты, поэтому точка доступа должна быть выполнена с шифрующим модулем. Передача данных по корпоративной локальной сети выполняется с использованием алгоритма шифрования. Шифрование осуществляется на аппаратном уровне, криптомодуль встроен в сетевой адаптер.
2.2 Создание виртуальных сетей. VLAN сформирована на базе 8 коммутаторов, все коммутаторы конфигурируются индивидуально, в соответствии с моделью доверия и бизнес-моделью.
2.3 На всех компьютерах устанавливаются списки непереносимой информации.
2.4 В соответствии с моделью пользовательских рисков, сформированной на базе обследования коллектива, для пользователей с высоким уровнем риска устанавливается программный продукт, осуществляющий теневое копирование.
2.5 На всех компьютерах корпоративной сети установлено специальное программно – аппаратное обеспечение, ограничивающее использование внешних носителей.
3. Защита периметра корпоративной сети от различных видов атак.
3.1 Разработать два объекта системы имитации уязвимости сетевых сервисов.
3.2 Объекты корпорации территориально разнесены и представляют собой совокупность автономных локальных сетей, с необходимостью объединения в корпоративную сеть, т.е. необходимостью создания VPN. Для создания VPN были провести следующие этапы:
3.2.1 Разбиение каждой из локальных сетей на сегменты - открытый сегмент для публичного доступа; сегмент внутренних серверов; сегмент внутренних рабочих мест; сегмент демилиторизованной зоны для формирования intranet и extranet.
3.2.2 Разработать настройки протокола IP и создать сервер безопасности, как один из промежуточных узлов маршрута.
3.2.3 В качестве intranet (extranet) – посредника разработать программно – аппаратный криптошлюз с алгоритмом туннелирования.
3.3 Для обеспечения контроля доступа к объектам корпоративной сети, разработать система firewall-ов. Схемы подключения и настройки выполнены в соответствии с моделью доверия и моделью рисков.
3.4 Выполнена система outsourcing. Для неё использовано стандартное программное обеспечение с индивидуальными настройками VPN для протокола IP.
3.5 В соответствии с моделью рисков и моделью доверия было сформирован комплекс антивирусной защиты.
3.6 Для реализации penetration-testing было разработано программное обеспечение теневого периодического сканирования сети.

Провести проверку предложенной системы безопасности на устойчивость к внутренним и внешним атакам, с привлечением сторонних организаций. По результаты проверки сделать обоснованный вывод о возможности внедрения системы безопасности на предприятие заказчика.

4. Методические материалы для определения процедур оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Промежуточная аттестация по дисциплине проводится в соответствии с требованиями СТП

СТО СПбГТИ(ТУ) 016-2015. КС УКДВ. Порядок проведения зачетов и экзаменов.

Виды учебных занятий. Курсовой проект. Курсовая работа. Общие требования : СТО СПбГТИ(ТУ) 044-2012 / СПбГТИ(ТУ). – Взамен СТП СПбГТИ 044-99 ; введ. с 01.06.2012. - СПб. : [б. и.], 2012. – 44 с.