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

УТВЕРЖДАЮ
Проректор по учебной
и методической работе
_____ Б.В.Пекаревский
«_____» _____ 2019 г.

Рабочая программа дисциплины

ИНТЕРНЕТ-ТЕХНОЛОГИИ

Направление подготовки

09.03.01 Информатика и вычислительная техника

Направленность 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

2019

Б1.О.19

ЛИСТ СОГЛАСОВАНИЯ

Должность разработчика	Подпись	Ученое звание, фамилия, инициалы
Доцент		А.С. Разыграев

Рабочая программа дисциплины «Интернет-технологии» обсуждена на заседании кафедры систем автоматизированного проектирования и управления
протокол от «18» апреля 2019 года № 9
Заведующий кафедрой Т.Б. Чистякова

Одобрено учебно-методической комиссией факультета информационных технологий и управления
протокол от «15» мая 2019 года № 9

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 учебно-методического управления		С.Н. Денисенко

СОДЕРЖАНИЕ

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

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения (дескрипторы)
ОПК-9 Способен осваивать методики использования программных средств для решения практических задач	**ОПК-9.2** Поиск и анализ технической документации по использованию программного средства, выбор и использование необходимых функций программных средств для решения конкретной задачи	**Знает:** Принципы и технологии глобальных сетей и сетей доступа. Сетевые операционные системы. Основные определения, классификацию и эксплуатационные характеристики локальных информационных сетей (ЗН-1). **Умеет:** - 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 (У-1). **Владеет:** - Навыками конфигурирования сетевого оборудования и программного обеспечения. Навыками использования современных программных средств (В-1).
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.3** Использование системных и прикладных программ для обеспечения безопасного и отказоустойчивого соединения с глобальной сетью Internet	**Знает:** типы подключения к глобальной сети; способы создания виртуально-независимого канала в глобальной сети (VPN); протоколы стека TCP/IP; Протоколы защищенной передачи данных (ЗН-2). **Умеет:** использовать системные и прикладные программы для обеспечения безопасного и отказоустойчивого соединения с глобальной сетью Internet (У-2). **Владеет:** методами проектирования защищенных корпоративных сетей и оценки их характеристик (В-2).

2. Место дисциплины в структуре образовательной программы.

Дисциплина «Интернет-технологии» относится к обязательной части Блока 1 «Дисциплины» образовательной программы бакалавриата (Б1.О.19) и изучается на 4 курсе на летней сессии и на 5 курсе на зимней сессии.

В методическом плане дисциплина опирается на элементы компетенций, сформированные при изучении дисциплин «Информатика», «История и перспективы развития информатики и вычислительной техники».

Полученные в процессе изучения дисциплины «Интернет-технологии» знания, умения и навыки могут быть использованы прохождении учебной, производственной и преддипломной практики, в научно-исследовательской работе студента и при выполнении выпускной квалификационной работы.

3. Объем дисциплины.

Вид учебной работы	Всего, академических часов	
	Заочная форма обучения	
	4 курс летняя сессия	5 курс зимняя сессия
Общая трудоемкость дисциплины (зачетных единиц/ академических часов)	1/36	3/108
Контактная работа с преподавателем:	**6**	**10**
занятия лекционного типа	6	
занятия семинарского типа, в т.ч.		
семинары, практические занятия		
лабораторные работы		6
курсовое проектирование (КП)		4
другие виды контактной работы		
Самостоятельная работа	**30**	**89**
Форма текущего контроля (Кр, реферат, РГР, эссе)		Кр (2 шт)
Форма промежуточной аттестации (КР, КП, зачет, экзамен)		КП, экзамен (9)

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	Формируемые индикаторы
			Семинары и/или практические занятия	Лабораторные работы			
1.	Аппаратное обеспечение и принципы функционирования корпоративных сетей	1	–	1	23	ОПК-3	ОПК-3.3
2.	Прикладные сервисы Intranet	1	–	1	23	ОПК-3	ОПК-3.3
3.	Алгоритмы маршрутизации корпоративных сетей	1	–	1	23	ОПК-3	ОПК-3.3
4.	Основы построения защищенных информационных систем	1	–	1	23	ОПК-9, ОПК-3	ОПК-3.3, ОПК-9.2
5.	Проектирование систем информационной безопасности корпоративных и промышленных сетей	2	–	2	27	ОПК-9, ОПК-3	ОПК-3.3, ОПК-9.2
	Итого по плану	6		6	119		

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	ЛВ
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	Л
3	Алгоритмы маршрутизации корпоративных сетей Протокол OSPF. Многокритериальность: надёжность, скорость, цена, уплотнение. Алгоритм Дейкстры. Таблицы маршрутизации. Маршрутизатор-мастер. Протокол RIP. Критерий маршрутизации. Формат кадра. Алгоритм работы.	1	Л
4	Основы построения защищенных информационных систем VPN. Принципы создания виртуально независимого канала интернет. Криптошлюз. Организация доступа через сервер безопасности. Демилитаризованная зона.	1	Л
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	Л

4.3. Занятия семинарского типа.

4.3.1. Семинары, практические занятия.

Не предусмотрены

4.3.2 Лабораторные занятия.

№ раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	Аппаратное обеспечение и принципы функционирования корпоративных сетей	1	-
2	Прикладные сервисы Intranet.	1	Интерактивные тренинги по выбору типа и конфигурации Firewall
3	Алгоритмы маршрутизации	1	Доклады, основанные на методике создания «кейсов»
4	Основы построения защищенных информационных систем	1	Применение методики развития критического мышления - ТРКМ
5	Проектирование систем информационной безопасности корпоративных сетей	2	Обсуждения индивидуально-ориентированных маршрутов, в контексте бакалаврской работы
	Итого:	6	

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 методы построения цифровых каналов.	23	Контрольная работа №1
2	Прикладные сервисы Intranet. Многоуровневые гетерогенные интерфейсы для организации обработки запроса клиента по протоколу http.	23	Контрольная работа №2
2,3	Алгоритмы маршрутизации. Особенности построения Российского сегмента.	23	Контрольная работа №2
4	Основы построения защищенных информационных систем. Аутентификация по биометрическим характеристикам.	23	Устный опрос
1	Проектирование систем информационной безопасности корпоративных сетей. Определение ущерба для корпорации, исходя из состава атакуемых данных. Создание системы дистанционного доступа к информационным ресурсам предприятия	27	Курсовой проект
	Итого:	119	Защита КП

4.5 Темы контрольных работ.

Предполагается написание студентами письменных трёх контрольных работ. ***Контрольные работы №1 и №2*** включают тестовые задания и выполняются с помощью прикладного программного обеспечения для тестирования знаний обучающихся с формированием соответствующего отчета (протокола обучения). Контрольные работы №1 и №2 выполняются студентами на 3 курсе после завершения изучения очередной темы или раздела дисциплины.

Контрольные работы посвящены следующей тематике:

Контрольная работа №1. Аппаратное обеспечение и принципы функционирования корпоративных сетей. Стандарты и методы построения цифровых каналов..

Контрольная работа №2. Прикладные сервисы Intranet. Многоуровневые гетерогенные интерфейсы для организации обработки запроса клиента по протоколу http. Алгоритмы маршрутизации. Особенности построения Российского сегмента..

Примеры тестовых заданий по Контрольным работам № 1-2:

Интернет-провайдер выделил адрес сети 206.73.118.0. В соответствии с вариантом определить и занести в таблицу

Количество бит, необходимое для идентификатора подсети	
Количество бит, необходимое для идентификатора узла	
Маска подсети в виде префикса сети	
Маска подсети в десятично-точечном виде	

Аргументировано ответить на вопрос, принадлежат ли два IP адреса к одной подсети. Маска подсети используется та же, что и в первом задании.

Корпоративная сеть использует адреса класса B и должна обеспечивать как минимум 1000 подсетей с 60 компьютерами в каждой.
Какая из приведенных масок для этого подходит?

1. 255.255.128.0
2. 255.255.240.0
3. 255.255.255.128
4. 255.255.255.192
5. 255.255.255.224

Маршрутизатор получает пакет с адресом назначения 172.16.59.179/22.
Какой подсети этот пакет адресован?

1. 172.16.56.0/22;
2. 172.16.59.0/22;
3. 172.16.48.0/22;
4. 172.16.32.0/22;
5. 172.16.56.48/22

Студенту необходимо представить слайд-презентацию с основными результатами контрольных работ, отчёт о выполненных контрольных работах в распечатанном виде и в электронном виде на любом носителе информации.

Отчёт должен включать: титульный лист, содержание работы, алгоритм решения (при необходимости) и результаты решения поставленной задачи. На титульном листе отчёта о выполнении контрольных работ необходимо указать фамилию, имя и отчество студента, номер учебной группы, номер контрольной работы.

По контрольным работам устанавливаются оценки «зачтено» или «не зачтено», формируемые по результатам представленных отчетов и устного собеседования.

Оценка «зачтено» ставится, если студент владеет необходимыми знаниями, умениями и навыками при выполнении контрольных заданий.

Оценка «не зачтено» ставится, если студент непоследователен в изложении результатов работ, не в полной мере владеет необходимыми умениями и навыками при выполнении контрольных заданий.

4.6. Темы курсовых проектов.

Целью курсового проекта является получение практических навыков создания систем дистанционного доступа к ресурсам предприятия с ограниченным числом пользователей..

Тематика курсового проекта – «Проектирование информационного портала предприятия с интерфейсом для дистанционного доступа к демилитаризованной информационной зоне, включающей серверный кластер. Разработка комплексной системы безопасности предприятия, включающей аппаратно-программные средства (appliance) и категорирование объектов и субъектов безопасности». Индивидуальные задачи конкретизируют типы предприятий и цели создания дистанционного доступа. Формирование задания на курсовое проектирование ведется с учетом будущей тематики выпускной квалификационной работы.

Содержание курсового проекта:

1.Проектирование системы дистанционного доступа к ресурсам предприятия (СДДРП)
1.1Назначение и область применения СДДРП
1.2Этапы проектирования СДДРП
1.1.1Архитектура СДДРП. Описание уровней и, входящих в их состав звеньев, СДДРП.
1.1.2 Сравнительный анализ существующих СДДРП в рассматриваемой области.

1.1.3Проектирование программного обеспечения для каждого уровня (звена) СДДРП
1.1.4Структура интерфейса СДДРП
1.1.3.1Топологическая схема ресурсов информационной части портала
1.1.3.2UML диаграммы пользователей, имеющих доступ к порталу
1.1.3.3Примеры интерфейсов СДДРП
1.1.3.4Этапы раскрутки СДДРП
Для обеспечения информационной безопасности корпорации разработать 3 составляющие:
Защита от несанкционированного доступа.

1. Регистрация: при доступе к серверу или использовании рабочих станций в качестве депозитария:
2. Ограничение прав доступа к объектам корпоративной сети через права и атрибуты: сформировать модель доверия: обследование коллектива сотрудников с целью выявления возможных инсайдеров; разбиение всей информации по классам защиты, в зависимости от важности информации и последствий её утечки.
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 использовать SAN.

Защита от внутренних нарушений политики безопасности.

1. Если в состав корпорации входят мобильные информационные объекты, точка доступа должна быть выполнена с шифрующим модулем.
2. Создание виртуальных сетей. VLAN должна быть сформирована на базе коммутаторов, все коммутаторы конфигурируются индивидуально, в соответствии с моделью доверия и бизнес-моделью.
3. На компьютерах корпоративной сети установить специальное программно – аппаратное обеспечение, ограничивающее использование внешних носителей.

Защита периметра корпоративной сети от различных видов атак.

1. Разработать и настроены два объекта системы имитации уязвимости сетевых сервесов.
2. Для обеспечения контроля доступа к объектам корпоративной сети, разработать система firewall-ов. Схемы подключения и настройки должны быть выполнены в соответствии с моделью доверия и моделью рисков.
3. В соответствии с моделью рисков и моделью доверия сформировать комплекс антивирусной защиты.

Сделать обоснованный вывод о возможности внедрения системы безопасности на предприятие заказчика.
Проектная документация проекта содержит: архитектуру СДДРП с подробным описанием уровней и, входящих в их состав звеньев; сравнительный анализ существующих СДДРП в рассматриваемой области; сравнительный анализ программного обеспечения, позволяющего реализовать каждый уровень (звено) СДДРП и обоснованный вывод о предпочтительном использовании.
Топологическую схему ресурсов информационной части портала. UML диаграммы пользователей, имеющих доступ к порталу. Примеры интерфейсов СДДРП, дополнительную сопроводительную документацию по указанию преподавателя.

Примерные темы курсового проекта:

1 Проектирование информационного портала предприятия «Приозерский хлебозавод» с интерфейсом для дистанционного доступа к демилитаризованной информационной зоне, включающей серверный кластер из четырех серверов для обеспечения приема

заказов. Разработка комплексной системы безопасности предприятия, включающей аппаратно-программные средства (appliance) и категорирование объектов и субъектов безопасности.

2 Проектирование информационного портала предприятия по производству промышленных смазок с интерфейсом для дистанционного доступа к демилитаризованной информационной зоне, включающей серверный кластер из двух серверов Баз Данных. Разработка комплексной системы безопасности предприятия, включающей аппаратно-программные средства (appliance) и категорирование объектов и субъектов безопасности.

Проектирование информационного портала частной школы с интерфейсом для дистанционного доступа к демилитаризованной информационной зоне, включающей серверный кластер из четырех серверов для обеспечения просмотра успеваемости. Разработка комплексной системы безопасности предприятия, включающей аппаратно-программные средства (appliance) и категорирование объектов и субъектов безопасности.

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 и защиты курсового проекта в зимней сессии на 5 курсе.

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

Экзамен предусматривает выборочную проверку освоения предусмотренных элементов компетенций и комплектуется двумя теоретическими вопросами для проверки знаний. Курсовой проект предусматривает проверку умений и навыков.

При сдаче экзамена студент получает два 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.

Фонд оценочных средств по дисциплине представлен в Приложении № 1.

Пример задания на выполнение курсового проекта приведен в Приложении № 2.

7. Перечень учебных изданий, необходимых для освоения дисциплины.

а) печатные издания:

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

2 Коваленко, В. В. Проектирование информационных систем : учеб. пособие для вузов / В. В. Коваленко. – М. : Форум, 2012. – 319 с.

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

4 Антонова, Г. М. Современные средства ЭВМ и телекоммуникаций : учеб. пособие для вузов / Г. М. Антонова, А. Ю. Байков. – М. : Академия, 2010. – 142 с.

5 Шевченко, В. П. Вычислительные системы, сети и телекоммуникации : учебник для вузов / В. П. Шевченко. – М. : КноРус, 2012. – 288 с.

6 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. – 519 с.

7 Мелехин, В. Ф. Вычислительные машины, системы и сети: учебник для вузов / В. Ф. Мелехин, Е. Г. Павловский. – 3-е изд. – М. : Academia, 2010. – 555 с.

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

б) электронные учебные издания:

9 Гельбух, С. С. Сети ЭВМ и телекоммуникации. Архитектура и организация: учеб. пособие / С. С. Гельбух. – СПб. ; М.; Краснодар : Лань, 2019. – 208 с. (ЭБС Лань)

10 Абросимов, Л. И. Базисные методы проектирования и анализа сетей ЭВМ: учеб. пособие / Л. И. Абросимов. – СПб.; М. ; Краснодар : Лань, 2018. – 212 с. (ЭБС Лань)

8. Перечень электронных образовательных ресурсов, необходимых для освоения дисциплины.

Рабочий учебный план подготовки бакалавров по программе бакалавриата направления подготовки 09.03.01 «Информатика и вычислительная техника», рабочая программа дисциплины и учебно-методические материалы по дисциплине размещены в электронной информационно-образовательной среде СПбГТИ(ТУ) на сайте Медиа по адресу: http://media.technolog.edu.ru.

Для подготовки к лабораторным и практическим занятиям, выполнения курсового проекта и самостоятельной работы студенты могут использовать следующие Интернет-ресурсы:

innovation.gov.ru (сайт об инновациях в России);

inftech.webservis.ru, citforum.ru (сайты информационных технологий);

www.novtex.ru/IT (веб-страница журнала «Информационные технологии»);

www.exponenta.ru (образовательный математический сайт);

model.exponenta.ru (сайт о моделировании и исследовании систем, объектов, технологических процессов и физических явлений);

prodav.exponenta.ru, sernam.ru (сайты по цифровой обработке сигналов);

www.gosthelp.ru/text/GOSTR507794096Statistiche, www.statsoft.ru/home/textbook/modules/stquacon (веб-страницы, посвященные методам и средствам мониторинга и контроля качества);

www.blackboard.com, bb.vpgroup.ru, moodle.org, websoft.ru/db/wb/root_id/webtutor, websoft.ru/db/wb/root_id/courselab (ресурсы, посвященные средам электронного обучения);

edu.ru (федеральный портал «Российское образование»);

www.openet.ru (российский портал открытого образования);

elibrary.ru (информационно-аналитический портал «Научная электронная библиотека»);

webofknowledge.com, scopus.com (международные мультидисциплинарные аналитические реферативные базы данных научных публикаций).

Электронно-библиотечные системы:

«Электронный читальный зал – БиблиоТех» (режим доступа: http://bibl.ltigti.ru/service1.html, вход по логину и паролю);

«Лань» (режим доступа: http://e.lanbook.com/books, свободный вход с любого зарегистрированного компьютера института).

9. Методические указания для обучающихся по освоению дисциплины.

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

Виды учебных занятий. Лекция. Общие требования : СТП СПбГТИ 040-02 / СПбГТИ(ТУ). – Введ. с 01.07.2002. – СПб. : [б. и.], 2002. – 7.00 с.

2 Виды учебных занятий. Лабораторные занятия. Общие требования к организации и проведению : СТП СПбГТИ 020-2011 / СПбГТИ(ТУ). – СПб. : [б. и.], 2011. – 21 с.

3 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.

4 Порядок проведения зачетов и экзаменов : СТП СПбГТИ 016-2015 / СПбГТИ(ТУ). – СПб. : [б. и.], 2015. – 21 с.

5 Виды учебных занятий. Самостоятельная планируемая работа студентов. Общие требования к организации и проведению : СТП СПбГТИ 048-2009 / СПбГТИ(ТУ). – Введ. с 01.01.2010. – СПб. : [б. и.], 2009. – 6 с.

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 знания 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 информационно-образовательной среды.

10.2. Программное обеспечение.

Операционная система Microsoft Windows 10 (подписка Azure Dev Tools for Teaching Subscription ID 1831112343).

Visual Studio Community (подписка Azure Dev Tools for Teaching Subscription ID 1831112343).

Visual Studio Enterprise (подписка Azure Dev Tools for Teaching Subscription ID 1831112343).

Pelles C (бесплатная лицензия).

Архиватор 7-zip (открытые лицензии (GNU LGPL, BSD 3-clause License, GNU LGP with unRAR license restriction)).

Moodle (открытая лицензия, GNU GPL v3).

Adobe Acrobat Reader DC (бесплатная лицензия «ADOBE Personal Computer Software License Agreement»).

LibreOffice (открытая лицензия, Mozilla Public License Version 2.0).

Бесплатные веб-браузеры: Google Chrome (Бесплатная некоммерческая лицензия), Mozilla Firefox (Открытая лицензия (Mozilla Public License V2)), Opera (Бесплатная лицензия (Opera EULA)).

10.3. Базы данных и информационные справочные системы.

Справочно-поисковая система «Консультант-Плюс»

Веб-страница журнала «Информационные технологии» http://www.novtex.ru/IT

Сайты информационных технологий: http://inftech.webservis.ru, http://citforum.ru

Информационно-аналитический портал «Научная электронная библиотека» http://elibrary.ru

Международные мультидисциплинарные аналитические реферативные базы данных научных публикаций http://webofknowledge.com, http://scopus.com

Электронно-библиотечные системы:

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

«Лань» https://e.lanbook.com/books/.

11. Материально-техническое обеспечение освоения дисциплины в ходе реализации образовательной программы.

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.

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 28.08.2014.

Приложение № 1
к рабочей программе дисциплины

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

1. Перечень компетенций и этапов их формирования.

Индекс компетенции	Содержание	Этап формирования
ОПК-9	Способен осваивать методики использования программных средств для решения практических задач	промежуточный
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	промежуточный

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

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
ОПК-9.2 Поиск и анализ технической документации по использованию программного средства, выбор и использование необходимых функций программных средств для решения конкретной задачи	Перечисляет принципы и технологии глобальных сетей и сетей доступа. Особенности и различия сетевые операционные системы. Основные определения, классификацию и эксплуатационные характеристики локальных информационных сетей (ЗН-1).	Ответы на вопросы №1, 31 к экзамену, КП	С ошибками называет определения, классификацию и эксплуатационные характеристики локальных информационных сетей.	Уверенно, но с небольшими ошибками называет определения, классификацию и эксплуатационные характеристики локальных информационных сетей.	Уверенно и без ошибок называет определения, классификацию и эксплуатационные характеристики локальных информационных сетей.
	Демонстрирует способность анализировать структуру корпоративной сети. Обосновать применение протоколов маршрутизации. Использовать прикладные протоколы и сервисы. Использовать стандартные протоколы стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе. Выполнять инсталляцию и первоначальную настройку сетевой ОС (У-1).	Ответы на вопросы №4, 30 к экзамену, КП	Объясняет с ошибками как выполнять базовые процедуры использования стандартные протоколы стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе.	Допускает небольшие ошибки в объяснении как выполнять базовые процедуры использования стандартные протоколы стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе.	Аргументировано объясняет, как выполнять базовые процедуры использования стандартные протоколы стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе.
	Объясняет методику конфигурирования сетевого оборудования и программного обеспечения. Демонстрирует владение навыками использования современных программных средств (В-1).	Ответы на вопрос №2 к экзамену, КП	Демонстрирует с ошибками и не все методики использования современных программных средств и конфигурирования сетевого оборудования.	Демонстрирует не все методики использования современных программных средств и конфигурирования сетевого оборудования.	Уверенно демонстрирует и правильно применяет методики использования современных программных средств и конфигурирования сетевого оборудования.
ОПК-3.3 Использование системных и прикладных	Перечисляет типы подключения к глобальной сети; способы создания виртуально-независимого	Ответы на вопросы №3, 5-14 к экзамену	Поверхностно и с ошибками рассказывает о способах создания	Уверенно, но с небольшими ошибками рассказывает о спосо-	Уверенно и без ошибок рассказывает о способах создания

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
программ для обеспечения безопасного и отказоустойчивого соединения с глобальной сетью Internet	канала в глобальной сети (VPN); протоколы стека TCP/IP; Протоколы защищенной передачи данных (ЗН-2).		виртуально-независимого канала в глобальной сети (VPN); протоколах стека TCP/IP; протоколах защищенной передачи данных.	бах создания виртуально-независимого канала в глобальной сети (VPN); протоколах стека TCP/IP; протоколах защищенной передачи данных.	виртуально-независимого канала в глобальной сети (VPN); протоколах стека TCP/IP; протоколах защищенной передачи данных.
	Рассказывает о возможности использовать системные и прикладные программы для обеспечения безопасного и отказоустойчивого соединения с глобальной сетью Internet (У – 2).	Ответы на вопросы №16, 18, 24-31 к экзамену	Осуществляет с ошибками выбор системного и прикладного программного обеспечения для безопасного и отказоустойчивого соединения с глобальной сетью Internet.	Осуществляет, допуская небольшие ошибки, выбор системного и прикладного программного обеспечения для безопасного и отказоустойчивого соединения с глобальной сетью Internet.	Осуществляет без ошибок выбор системного и прикладного программного обеспечения для безопасного и отказоустойчивого соединения с глобальной сетью Internet.
	Демонстрирует методики выбора проектных решений для создания защищенных корпоративных сетей и оценки их характеристик (В -2).	Ответы на вопросы №15, 17, 19, 20-23, 32-54 к экзамену	Демонстрирует с ошибками и не все методики выбора проектных решений для создания защищенных корпоративных сетей и оценки их характеристик.	Демонстрирует не все методики выбора проектных решений для создания защищенных корпоративных сетей и оценки их характеристик.	Уверенно демонстрирует и правильно применяет методики выбора проектных решений для создания защищенных корпоративных сетей и оценки их характеристик.

3. Типовые контрольные задания для проведения промежуточной аттестации

Вопросы для оценки знаний, умений и навыков, сформированных у студента по компетенциям:

Номер вопроса	Вопрос	Компетенция
1	Принципы построения отказоустойчивых систем.	ОПК-9
2	Парадигмы семейства протоколов TCP/IP.	ОПК-9
3	Структура объединенной компьютерной сети образования, науки и культуры.	ОПК-3
4	Основные задачи proxy- сервера	ОПК-9
5	Сетевая файловая система.	ОПК-3
6	DHCP- протокол.	ОПК-3
7	Метод трансляции сетевого адреса.	ОПК-3
8	Кадр протокола DNS.	ОПК-3
9	Компоненты информационных сетей; методы коммутации; непрерывный и дискретный каналы связи.	ОПК-3
10	Методы защиты от ошибок и обеспечения безопасности информации.	ОПК-3
11	Оценки характеристик защищенных сетей.	ОПК-3
12	Способы создания виртуально-независимого канала в глобальной сети (VPN).	ОПК-3
13	Протоколы защищенной передачи данных IPSec, SSL/TLS.	ОПК-3
14	Протоколы маршрутизации в IP-сетях и их характеристики.	ОПК-3
15	Методы и средства информационных сетей при создании комплексов обработки информации.	ОПК-3
16	Методы защиты от ошибок и обеспечения отказоустойчивости информационных систем.	ОПК-3
17	Непрерывный и дискретный каналы связи.	ОПК-3
18	Характеристики протоколов маршрутизации в корпоративных сетях.	ОПК-3
19	Методика проектирования защищенных корпоративных сетей.	ОПК-3
20	Принципы проектирования распределенных систем управления.	ОПК-3
21	Протоколы стека TCP/IP.	ОПК-3
22	Протоколы маршрутизации в IP-сетях и их характеристики.	ОПК-3
23	Средства информационных сетей при создании комплексов обработки информации.	ОПК-3
24	Методы защиты от ошибок при передачи данных в глобальной сети.	ОПК-3
25	Коммутация сообщений.	ОПК-3
26	Алгоритмы межсетевого обмена данными.	ОПК-3
27	Синхронная и асинхронная передача.	ОПК-3
28	Гибридные системы.	ОПК-3
29	Классификация промышленных сетей с дистанционным доступом.	ОПК-3
30	Классификация методов доступа.	ОПК-3, ОПК-9
31	Аппаратное обеспечение промышленных сетей с дистанци-	ОПК-3, ОПК-9

	онным доступом.	
32	Службы совместного использования информации.	ОПК-3
33	Мостовые соединения. Повторители, шлюзы, коммутаторы. Краткое описание функций мостов и маршрутизаторов.	ОПК-3
34	Классификация протоколов.	ОПК-3
35	Протокол IPX.	ОПК-3
36	Семейство протоколов TCP/IP: Протокол IP и ARP.	ОПК-3
37	Семейство протоколов TCP/IP: Протокол TCP и UDP.	ОПК-3
38	Режимы функционирования ВС. Мультипрограммный режим. Понятие параллельных процессов.	ОПК-3
39	Многозадачная работа и системы реального времени.	ОПК-3
40	Понятие и структура интерфейсов ЭВМ. Системные интерфейсы ЭВМ.	ОПК-3
41	Интернет-провайдер выделил адрес сети 206.73.118.0. Количество требуемых подсетей или узлов – 6 подсетей. Определить и занести в таблицу: количество бит, необходимое для идентификатора подсети; количество бит, необходимое для идентификатора узла; маска подсети в виде префикса сети; маска подсети в десятично-точечном виде.	ОПК-3
42	Для IP адреса 140.31.26.112 и маски подсети 255.255.240.0 определить и занести в таблицу: адрес подсети; минимальный адрес в сети; максимальный адрес в сети; броадкаст адрес сети; возможное количество подсетей; количество адресов сети, которое можно назначить компьютерам сети.	ОПК-3
43	Интерфейсы периферийных устройств.	ОПК-3
44	Интерфейсы сетей ЭВМ.	ОПК-3
45	Назначение, физические принципы работы и параметры внешних устройств ЭВМ.	ОПК-3
46	Назначение, физические принципы работы и параметры внешних устройств ЭВМ.	ОПК-3
47	Назначение, физические принципы работы и параметры внешних устройств ЭВМ: интерактивные, мультимедийные устройства.	ОПК-3
48	Методы создания отказоустойчивой сети хранения данных.	ОПК-3
49	Оптимизация использования вычислительных мощностей и дискового пространства при использовании механизма виртуализации.	ОПК-3
50	Методы минимизации угроз.	ОПК-3
51	Эксплуатационные характеристики ЭВМ. Показатели производительности и надежности.	ОПК-3
52	Методы и средства повышения надежности в вычислительных сетях.	ОПК-3
53	Виды кластеров. Аппаратные и программные кластеры.	ОПК-3
54	Виртуальные сети (VLAN).	ОПК-3

При сдаче экзамена, студент получает два вопроса из перечня, приведенного выше.

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

4. Методические материалы для определения процедур оценивания знаний, умений и навыков, характеризующих этапы формирования компетенций.

Промежуточная аттестация по дисциплине проводится в соответствии с требованиями СТО СПбГТИ(ТУ) 016-2015. КС УКДВ Порядок организации и проведения зачетов и экзаменов.

Приложение № 2

к рабочей программе дисциплины

Минобрнауки России
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный технологический институт
(технический университет)»

ЗАДАНИЕ НА КУРСОВОЙ ПРОЕКТ ПО ДИСЦИПЛИНЕ «ИНТЕРНЕТ ТЕХНОЛОГИИ»

Направление подготовки	09.03.01	Информатика и вычислительная техника
Направленность программы бакалавриата		Автоматизированные системы обработки информации и управления
Факультет		Информационных технологий и управления
Кафедра		Систем автоматизированного проектирования и управления

Студент_____ группы____

Тема Проектирование информационного портала и системы информационной безопасности корпоративной сети предприятия «___».

Цель работы Проектирование информационного портала предприятия с интерфейсом для дистанционного доступа к демилитаризованной информационной зоне, включающей _____ Разработка комплексной системы безопасности предприятия_____, включающей аппаратно-программные средства (appliance) и категорирование объектов и субъектов безопасности.

Исходные данные к работе

а) основная литература:

1. 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.
2. Хорошевский, В. Г. Архитектура вычислительных систем : учеб. пособие для вузов / В. Г. Хорошевский. – 2-е изд. – М. : Изд-во МГТУ им. Н.Э.Баумана, 2011. – 520 с.

б) дополнительная литература:

3. 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, 2012. – 552 с.
4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : учеб. пособие для вузов / В. Ф. Шаньгин. – М. : ДМК-Пресс, 2012. – 542 с.

в) вспомогательная литература:

5. Платонов,В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей:учеб. пособие для вузов / В. В. Платонов. –М. : Академия, 2013. – 239 с.
6. Ресурсы электронно-библиотечной системы «Электронный читальный зал – Библиотех»:
7. Избачков, Ю. Информационные системы : учеб. для вузов / Ю. Избачков. – 3-е изд. – СПб. : Питер, 2010. – 544 с.

Основное содержание работы:

1.Проектирование системы дистанционного доступа к ресурсам предприятия (СДДРП)
1.1Назначение и область применения СДДРП
1.2Этапы проектирования СДДРП
1.1.1Архитектура СДДРП. Описание уровней и, входящих в их состав звеньев, СДДРП.
1.1.2 Сравнительный анализ существующих СДДРП в рассматриваемой области.
1.1.3Проектирование программного обеспечения для каждого уровня (звена) СДДРП
1.1.4Структура интерфейса СДДРП
1.1.3.1Топологическая схема ресурсов информационной части портала
1.1.3.2UML диаграммы пользователей, имеющих доступ к порталу
1.1.3.3Примеры интерфейсов СДДРП

1.1.3.4Этапы раскрутки СДДРП

Для обеспечения информационной безопасности корпорации разработать 3 составляющие:

Защита от несанкционированного доступа.

4. Регистрация: при доступе к серверу или использовании рабочих станций в качестве депозитария:
    a. Обеспечить двустороннюю идентификацию клиентов; при успешном прохождении - одностороннюю идентификацию пользователя.
    b. На этапе аутентификации предложить механизм генерации одноразовых паролей с периодическим сканированием (при запросе доступа к ключевым источникам информации) биометрических характеристик (стандартные аппаратные средства сканирования).
    c. Авторизацию осуществить времянными рамками входа. При запросах к удаленному компьютеру, дополнить ограничением числа сеансов одного и того же пользователя. При запросе доступа к ключевому источнику информации - ограничением времени использования.
5. Ограничение прав доступа к объектам корпоративной сети через права и атрибуты: сформировать модель доверия: обследование коллектива сотрудников с целью выявления возможных инсайдеров; разбиение всей информации по классам защиты, в зависимости от важности информации и последствий её утечки.
6. 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 использовать SAN.

Защита от внутренних нарушений политики безопасности.

4. Если в состав корпорации входят мобильные информационные объекты, точка доступа должна быть выполнена с шифрующим модулем.
5. Создание виртуальных сетей. VLAN должна быть сформирована на базе коммутаторов, все коммутаторы конфигурируются индивидуально, в соответствии с моделью доверия и бизнес-моделью.
6. На компьютерах корпоративной сети установить специальное программно – аппаратное обеспечение, ограничивающее использование внешних носителей.

Защита периметра корпоративной сети от различных видов атак.

4. Разработать и настроены два объекта системы имитации уязвимости сетевых сервесов.
5. Для обеспечения контроля доступа к объектам корпоративной сети, разработать система firewall-ов. Схемы подключения и настройки должны быть выполнены в соответствии с моделью доверия и моделью рисков.
6. В соответствии с моделью рисков и моделью доверия сформировать комплекс антивирусной защиты.

Сделать обоснованный вывод о возможности внедрения системы безопасности на предприятие заказчика.

Перечень графического материала

Схема системы комплексной информационной безопасности корпоративной сети

Схема виртуальной коммутируемой сети

Схема расположения firewalls

Схема расположенияhoneypots

Характеристика программного и аппаратного обеспечений.

Дата выдачи задания “___” _____ 20___

Дата представления работы к защите “____” _____ 20____

Заведующий кафедрой

Профессор Т.Б. Чистякова

Руководитель

Доцент А.С. Разыграев

Задание принял к выполнению_____