

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Пекаревский Борис Владимирович  
Должность: Проректор по учебной и методической работе  
Дата подписания: 30.05.2022 15:05:34  
Уникальный программный ключ:  
3b89716a1076b80b2c167df0f27c09d01782ba84



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**

Направленности программы бакалавриата

**Системы автоматизированного проектирования**

**Автоматизированные системы обработки информации и управления**

Квалификация

**Бакалавр**

Форма обучения

**Очная**

Факультет **информационных технологий и управления**

Кафедра **систем автоматизированного проектирования и управления**

Санкт-Петербург  
2019

**Б1.О.19**

## ЛИСТ СОГЛАСОВАНИЯ

Должность	Подпись	Ученое звание, инициалы, фамилия
Старший преподаватель		О. Г. Новикова

Рабочая программа дисциплины «Интернет-технологии» обсуждена на заседании кафедры систем автоматизированного проектирования и управления  
протокол от «18» апреля 2019 № 9

Заведующий кафедрой

Т.Б. Чистякова

Одобрено учебно-методической комиссией факультета информационных технологий и управления,  
протокол от «15» мая 2019 № 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 УМУ		С.Н. Денисенко

## СОДЕРЖАНИЕ

1	Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы .....	4
2	Место дисциплины в структуре образовательной программы .....	5
3	Объем дисциплины.....	5
4	Содержание дисциплины.....	6
4.1	Разделы дисциплины и виды занятий .....	6
4.2	Занятия лекционного типа .....	7
4.3	Занятия семинарского типа .....	8
4.3.1	Семинары, практические занятия.....	8
4.3.2	Лабораторные занятия .....	8
4.4	Самостоятельная работа обучающихся.....	9
4.5	Темы и содержание контрольных работ .....	9
4.6	Темы курсовых проектов.....	11
5	Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине .....	13
6	Фонд оценочных средств для проведения промежуточной аттестации .....	14
7	Перечень учебных изданий, необходимых для освоения дисциплины .....	15
8	Перечень электронных образовательных ресурсов, необходимых для освоения дисциплины.....	16
9	Методические указания для обучающихся по освоению дисциплины.....	17
10	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине .....	18
10.1	Информационные технологии.....	18
10.2	Программное обеспечение.....	18
10.3	Базы данных и информационные справочные системы .....	19
11	Материально-техническое обеспечение освоения дисциплины в ходе реализации образовательной программы .....	19
12	Особенности освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья .....	20

Приложения: 1 Фонд оценочных средств для проведения промежуточной аттестации

2 Шаблон задания на курсовой проект

**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:

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

## 2 Место дисциплины в структуре образовательной программы

Дисциплина «Интернет-технологии» относится к дисциплинам обязательной части (Б1.О.19) и изучается на 3 курсе в 6 семестре.

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

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

## 3 Объем дисциплины

Вид учебной работы	Всего, ЗЕ/академ. часов
<b>Общая трудоемкость дисциплины</b> (зачетных единиц/ академических часов)	<b>4/ 144</b>
<b>Контактная работа с преподавателем:</b>	<b>65</b>
занятия лекционного типа	16
занятия семинарского типа, в т.ч.	30
семинары, практические занятия	–
лабораторные работы	30
курсовое проектирование (КР или КП)	15
КСР	4
другие виды контактной работы	–
<b>Самостоятельная работа</b>	<b>43</b>
<b>Форма текущего контроля</b> (Кр, реферат, РГР, эссе)	3 Кр
<b>Форма промежуточной аттестации</b> (КР, КП, зачет, экзамен)	<b>КП, Экзамен/36</b>

## 4 Содержание дисциплины

### 4.1 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Занятия лекционного типа, академ. часы	Занятия семинарского типа, академ. часы		Самостоятельная работа, академ. часы	Формируемые компетенции	Формируемые индикаторы
			Семинары и/или практические занятия	Лабораторные работы			
1.	Аппаратное обеспечение и принципы функционирования корпоративных сетей	4	–	8	4	ОПК-3	ОПК-3.3
2.	Прикладные сервисы Intranet	3	–	6	4	ОПК-3	ОПК-3.3
3.	Алгоритмы маршрутизации корпоративных сетей	3	–	6	4	ОПК-3	ОПК-3.3
4.	Основы построения защищенных информационных систем	3	–	6	7	ОПК-9, ОПК-3	ОПК-3.3, ОПК-9.2
5.	Проектирование систем информационной безопасности корпоративных и промышленных сетей	3	–	4	24	ОПК-9, ОПК-3	ОПК-3.3, ОПК-9.2
	<b>Итого:</b>	<b>16</b>		<b>30</b>	<b>43</b>		

#### 4.2 Занятия лекционного типа

№раздела дисциплины	Наименование темы и краткое содержание занятия	Объем, акад. часы	Инновационная форма
1	<b>Аппаратное обеспечение и принципы функционирования корпоративных сетей</b> Структура глобальной сети. Перспективы развития, основные направления новых исследований. Функции федеральных, региональных и местных узлов. Определение провайдера. Необходимое оборудование. Виды услуг и сервисов провайдера.	4	Лекция-визуализация
2	<b>Прикладные сервисы Intranet.</b> Протокол RARP, как предшественник протокола DHCP. Протокол DHCP. Система DNS. Первичный и вторичный сервера DNS. Реверсные запросы. <b>Сервис электронной почты.</b> Пользовательский клиент – функции, алгоритм работы. Транспортный агент. Доставочный агент.	3	Традиционная лекция
3	<b>Алгоритмы маршрутизации корпоративных сетей</b> Протокол OSPF. Многокритериальность: надёжность, скорость, цена, уплотнение. Алгоритм Дейкстры. Таблицы маршрутизации. Маршрутизатор-мастер. Протокол RIP. Критерий маршрутизации. Формат кадра. Алгоритм работы.	3	Традиционная лекция
4	<b>Основы построения защищенных информационных систем</b> VPN. Принципы создания виртуально независимого канала интернет. Криптошлюз. Организация доступа через сервер безопасности. Демилитаризованная зона.	3	Традиционная лекция
5	<b>Проектирование систем информационной безопасности корпоративных сетей</b> 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	3	Традиционная лекция
	Итого:	16	–

### 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	8	-
2	Прикладные сервисы Intranet.	6	Интерактивные тренинги по выбору типа и конфигурации Firewall
3	Алгоритмы маршрутизации	6	Доклады, основанные на методике создания «кейсов»
4	Основы построения защищенных информационных систем	6	Применение методики развития критического мышления - ТРКМ
5	Проектирование систем информационной безопасности корпоративных сетей	4	Обсуждения индивидуально-ориентированных маршрутов, в контексте бакалаврской работы
	Итого:	30	



#### 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.	4	Контрольная работа №1
2	Прикладные сервисы Intranet. Многоуровневые гетерогенные интерфейсы для организации обработки запроса клиента по протоколу http.	4	Контрольная работа №2
2,3	Алгоритмы маршрутизации. Особенности построения Российского сегмента.	4	Контрольная работа №3
4	Основы построения защищенных информационных систем. Аутентификация по биометрическим характеристикам.	7	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	24	Курсовой проект
	Итого:	43	Защита КП

#### 4.5 Темы и содержание контрольных работ

Предполагается написание студентами письменных трёх контрольных работ. **Контрольные работы №1, №2 и №3** включают тестовые задания и выполняются с помощью прикладного программного обеспечения для тестирования знаний обучающихся с формированием соответствующего отчета (протокола обучения). Контрольные работы №1, №2 и №3 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.

**Контрольная работа №3.** Алгоритмы маршрутизации. Особенности построения Российского сегмента..

Примеры тестовых заданий по Контрольным работам № 1-3:

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 адресак одной подсети. Маска подсети используется та же, что и в первом задании.

Корпоративная сеть использует адреса класса В 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 выпол-

нении контрольных заданий.

## 4.6 Темы курсовых проектов

### Темы и содержание курсового проекта

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

пасности.

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.

3 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 обучающимися 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 6 семестре.

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

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

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

Пример варианта вопросов на экзамене:

<b>Вариант № 1</b>
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.

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.-555с.
- 8 Платонов, В.В. Программно – аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие для вузов /В.В. Платонов. – М.: Академия, 2006. – 239с

### *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. – 208с. (ЭБС Лань)
- 10 Абросимов, Л.И. Базисные методы проектирования и анализа сетей ЭВМ: учеб. пособие /Л.И. Абросимов. – СПб.; М.; Краснодар: Лань, 2018. – 212с. (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](http://innovation.gov.ru) (сайт об инновациях в России);
  - [inftech.webservis.ru](http://inftech.webservis.ru), [citforum.ru](http://citforum.ru) (сайты информационных технологий);
  - [www.novtex.ru/IT](http://www.novtex.ru/IT) (веб-страница журнала «Информационные технологии»);
  - [www.exponenta.ru](http://www.exponenta.ru) (образовательный математический сайт);
  - [model.exponenta.ru](http://model.exponenta.ru) (сайт о моделировании и исследовании систем, объектов, технологических процессов и физических явлений);
  - [prodav.exponenta.ru](http://prodav.exponenta.ru), [sernam.ru](http://sernam.ru) (сайты по цифровой обработке сигналов);
  - [www.gosthelp.ru/text/GOSTR507794096Statistiche](http://www.gosthelp.ru/text/GOSTR507794096Statistiche),  
[www.statsoft.ru/home/textbook/modules/stquacon](http://www.statsoft.ru/home/textbook/modules/stquacon) (веб-страницы, посвященные методам и средствам мониторинга и контроля качества);
  - [www.blackboard.com](http://www.blackboard.com), [bb.vpgroup.ru](http://bb.vpgroup.ru), [moodle.org](http://moodle.org), [websoft.ru/db/wb/root\\_id/webtutor](http://websoft.ru/db/wb/root_id/webtutor),  
[websoft.ru/db/wb/root\\_id/courselab](http://websoft.ru/db/wb/root_id/courselab) (ресурсы, посвященные средам электронного обучения);
  - [edu.ru](http://edu.ru) (федеральный портал «Российское образование»);
  - [www.openet.ru](http://www.openet.ru) (российский портал открытого образования);
  - [elibrary.ru](http://elibrary.ru) (информационно-аналитический портал «Научная электронная библиотека»);
  - [webofknowledge.com](http://webofknowledge.com), [scopus.com](http://scopus.com) (международные мультидисциплинарные аналитические реферативные базы данных научных публикаций).
- Электронно-библиотечные системы:
- «Электронный читальный зал – БиблиоТех» (режим доступа: <http://bibl.lti-gti.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

Преподавание настоящей дисциплины предусматривает подробное изучение принципов построения отказоустойчивых и распределенных вычислительных систем, соответствующих заданному уровню информационной безопасности. Именно это позволит студентам в дальнейшем обоснованно решать стандартные задачи профессиональной деятельности, принимать участие во внедрении, адаптации и настройке вычислительных систем и сетей различного назначения, а также приобрести некоторые навыки в их разработке и сопровождении.

Занятия по дисциплине необходимо проводить в соответствии с требованиями стандартов:

1 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 лабораторных занятиях после выполнения лабораторных работ студенты с использованием компьютеров и соответствующего программного обеспечения подготавливают соответствующие отчеты.

Защиту курсового проекта по дисциплине следует проводить с применением мультимедийной техники с целью демонстрации разработанного программного обеспечения и презентационного материала.

Промежуточная аттестация по дисциплине осуществляется в конце семестра в виде зачета или экзамена, проводимого в устной форме, а также выполнения курсового проекта.

Необходимым условием получения допуска к зачету или экзамену является выпол-

нение и защита студентом всех лабораторных работ, предусмотренных рабочей программой.

При подготовке к зачету или экзамену рекомендуется несколько раз прочитать конспект лекций, дополненный информацией из рекомендуемых источников. При этом студент, поняв логику изложения учебного материала, получает представление о предмете изучаемой дисциплины в целом, что позволяет ему продемонстрировать на экзамене свои знания и эрудицию.

На экзамене студент отвечает в устной форме на два контрольных вопроса из различных разделов дисциплины. Список контрольных вопросов для проведения экзамена представлен в Приложении № 1. Оценка («неудовлетворительно», «удовлетворительно», «хорошо», «отлично»), формируемая в результате собеседования, является итоговой по дисциплине и проставляется в приложении к диплому.

Оценка за курсовой проект («неудовлетворительно», «удовлетворительно», «хорошо», «отлично»), формируемая по результатам публичной защиты и демонстрации разработанного программного обеспечения и презентационного материала, является так же итоговой по дисциплине и проставляется в приложении к диплому.

## **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 MicrosoftWindows 10.

Отечественная операционная система CalculateLinux.

Отечественное антивирусное программное обеспечение KasperskyEndpointSecurity.

Архиватор 7Zip.

СДО Moodle.

Adobe Acrobat Reader.

LibreOffice.

Бесплатные веб-браузеры: Google Chrome/Mozilla Firefox/Opera).  
 Среда виртуализации Oracle VirtualBOX.  
 Медиапроигрыватель VLC.  
 CM-1800. Бесплатное лицензионное соглашение.

### 10.3 Базы данных и информационные справочные системы

Web of Science (режим доступа: <http://apps.webofknowledge.com>, свободный с любого зарегистрированного компьютера института).

Scopus (режим доступа: <http://www.scopus.com>, свободный с любого зарегистрированного компьютера института).

Справочно-поисковая система «КонсультантПлюс: Высшая школа» (режим доступа: <http://www.consultant.ru/hs>, свободный с любого зарегистрированного компьютера института).

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

Наименование помещений	Оснащенность помещений
Лекционные кабинеты: 190013, г. Санкт-Петербург, Московский проспект, д. 24-26/49, лит. А, 1 этаж, помещение 41Н., пом. №5.	Лекционная аудитория оснащена средствами мультимедиа, интерактивной доской, мебелью, вместимость 60 посадочных мест (мультимедийная интерактивная доска ScreenMedia; ноутбуки Asus и Sony VarioVPCSA; проекторы NEC NP40 и Benq MS524)
Учебные аудитории для проведения занятий семинарского и практического типа, курсового проектирования (выполнения курсовых работ), для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: 190013, г. Санкт-Петербург, Московский проспект, д. 24-26/49, лит. А, 1 этаж, помещение 41Н., пом. №№ 4, 7, 8, 12	Персональные компьютеры объединены в локальную вычислительную сеть кафедры, имеют выход в сеть Интернет и обеспечивают доступ в электронную информационно-образовательную среду СПбГТИ(ТУ). Класс интегрированных систем проектирования и управления технологическими процессами: Персональные компьютеры (15 шт.): двухъядерный 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. Промышленный контроллер Unitronics M90 Micro OPCL, включаемый в состав лабораторного комплекса для обучения современным средствам разработки автоматизи-

	<p>зированных рабочих мест операторов технологических процессов, проектирования систем управления нижнего уровня. Программно-аппаратный комплекс, состоящий из учебного трехкоординатного фрезерно-гравировального станка с числовым программным управлением «Снайпер 8», предназначенного для выполнения операций по обработке легкообрабатываемых материалов, и персонального компьютера на базе процессора AMD Sempron, на котором установлена среда проектирования Adem для построения трехмерных геометрических моделей деталей, изготавливаемых на станке.</p> <p>Класс информационных и интеллектуальных систем:</p> <p>Персональные компьютеры (20 шт.): четырехядерный процессор IntelCore 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.</p> <p>Класс моделирования и оптимизации сложных технических систем:</p> <p>Персональные компьютеры (9 шт.): моноблок Lenovo C360 с 19,5-дюймовым дисплеем; процессор IntelCore i3-4130T (2,9ГГц); ОЗУ 4 Гб; НЖМД 1000 Гб; встроенные DVD-RW, видеокарта Intel HD Graphics 4400, звуковая и сетевая карты.</p>
--	---

## **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.

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

**1. Перечень компетенций и этапов их формирования**

<b>Индекс компетенции</b>	<b>Содержание</b>	<b>Этап формирования</b>
<b>ОПК-9</b>	Способен осваивать методики использования программных средств для решения практических задач	промежуточный
<b>ОПК-3</b>	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)
<b>ОПК-9.2</b> 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.	Ответы на вопросы №4, 30 к экзамену, КП	Объясняет с ошибками как выполнять базовые процедуры использования стандартных протоколов стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе.	Допускает небольшие ошибки в объяснении как выполнять базовые процедуры использования стандартных протоколов стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе.	Аргументированно объясняет как выполнять процедуры использования стандартных протоколов стека TCP/IP для организации сетевого взаимодействия приложений в распределенной системе.

Продолжение приложения №1

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
	ствия приложений в распределенной системе. Выполнять установку первоначальную настройку сетевой ОС. (У-1)			ленной 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 правильно применение современных программных средств и конфигурирование сетевого оборудования.
<b>ОПК-3.3</b> Использование системных и прикладных программ для обеспечения безопасного и отказоустойчивого	Перечисляет типы подключения к глобальной сети; способы создания виртуально-независимого канала в глобальной сети (VPN); протоколы стека TCP/IP; Протоколы защищенной передачи данных. (ЗН-2)	Ответы на вопросы №3, 5-14 к экзамену	Поверхностно и с ошибками рассказывает о способах создания виртуально-независимого канала в глобальной сети (VPN); протоколах стека TCP/IP; протоколах защищенной передачи данных.	Уверенно, но с небольшими ошибками рассказывает о способах создания виртуально-независимого канала в глобальной сети (VPN); протоколах стека TCP/IP; протоколах защищенной передачи данных.	Уверенно и подробно рассказывает о способах создания виртуально-независимого канала в глобальной сети (VPN); протоколах стека TCP/IP; протоколах защищенной передачи данных.

Продолжение приложения №1

Код и наименование индикатора достижения компетенции	Показатели сформированности (дескрипторы)	Критерий оценивания	Уровни сформированности (описание выраженности дескрипторов)		
			«удовлетворительно» (пороговый)	«хорошо» (средний)	«отлично» (высокий)
соединения с глобальной сетью Internet	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 выбор системного и прикладного программного обеспечения для безопасного и отказоустойчивого соединения с 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 правильно методики выбора проектных решений для создания защищенных корпоративных сетей и оценки их характеристик

Шкала оценивания соответствует СТО СПбГТИ(ТУ):

По дисциплине промежуточная аттестация проводится в форме экзамена и защиты курсового проекта, шкала оценивания – балльная («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»).



### 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-9
4	Основные задачи проху- сервера	ОПК-9
5	Сетевая файловая система.	ОПК-3
6	DHCP- протокол.	ОПК-3
7	Метод трансляции сетевого адреса.	ОПК-9, ОПК-3
8	Кадр протокола DNS.	ОПК-9
9	Компоненты информационных сетей; методы коммутации; непрерывный и дискретный каналы связи	ОПК-3
10	методы защиты от ошибки обеспечения безопасности информации;	ОПК-9
11	оценки характеристик защищенных сетей	ОПК-9
12	способы создания виртуально-независимого канала в глобальной сети (VPN);	ОПК-9
13	протоколы защищенной передачи данных IPSec, SSL/TLS	ОПК-9
14	протоколы маршрутизации в IP-сетях и их характеристики;	ОПК-9
15	методы и средства информационных сетей при создании комплексов обработки информации	ОПК-9
16	методы защиты от ошибок и обеспечения отказоустойчивости информационных систем	ОПК-9
17	непрерывный и дискретный каналы связи	ОПК-9
18	Характеристики протоколов маршрутизации в корпоративных сетях	ОПК-9
19	методика проектирования защищенных корпоративных сетей	ОПК-9
20	Принципы проектирования распределенных систем управления.	ОПК-9
21	протоколы стека TCP/IP;	ОПК-9
22	протоколы маршрутизации в IP-сетях и их характеристики;	ОПК-9
23	средства информационных сетей при создании комплексов обработки информации	ОПК-9
24	Знает методы защиты от ошибок при передаче данных в глобальной сети	ОПК-3
25	Коммутация сообщений.	ОПК-3
26	Алгоритмы межсетевого обмена данными	ОПК-3

Продолжение приложения №1

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
31	Аппаратное обеспечение промышленных сетей с дистанционным доступом.	ОПК-3
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; бродкаст 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	ОПК-3

Продолжение приложения №1

	устройства.	
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.

**5 Методические материалы для определения процедур оценивания знаний, умений и навыков, 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.

## Продолжение приложения №2

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		Системы автоматизированного проектирования 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 – Библиотека»:

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)

1.1 Назначение и область применения СДДРП

1.2 Этапы проектирования СДДРП

1.1.1 Архитектура СДДРП. Описание уровней и, входящих в их состав звеньев, СДДРП.

## Продолжение приложения №2

- 1.1.2 Сравнительный анализ существующих СДДРП в рассматриваемой области.
- 1.1.3 Проектирование программного обеспечения для каждого уровня (звена) СДДРП
- 1.1.4 Структура интерфейса СДДРП
  - 1.1.3.1 Топологическая схема ресурсов информационной части портала
  - 1.1.3.2 UML диаграммы пользователей, имеющих доступ к portalу
  - 1.1.3.3 Примеры интерфейсов СДДРП
  - 1.1.3.4 Этапы 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 временными 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 сервисов.
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 расположения honeypots
- Характеристика программного и аппаратного обеспечений.

## Продолжение приложения №2

1.

Дата выдачи задания “\_\_\_” \_\_\_\_\_ 20\_\_\_

Дата представления работы к защите “\_\_\_” \_\_\_\_\_ 20\_\_\_

Заведующий кафедрой

Профессор

Руководитель

Ст. преподаватель

Задание принял к выполнению \_\_\_\_\_

Т.Б. Чистякова

О.Г. Новикова