МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
информационных систем

Э.К. Алгазинов
29.06.2018

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.03.01 Информационная безопасность интранет-сетей

1. Шифр и наименование направления подготовки/специальности:
09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализации: *Анализ и синтез информационных систем. Безопасность информационных систем.*

3. Квалификация (степень) выпускника: *магистр*

4. Форма образования: *очная*

5. Кафедра, отвечающая за реализацию дисциплины: *Информационных систем*

6. Составители программы:
Коваль Андрей Сергеевич, koval@cs.vsu.ru, ст.преп, факультет компьютерных наук, кафедра информационный систем

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол № 6 от 25.06.2018

8. Учебный год: 2018-2019 **Семестр(ы): 2**

9. Цели и задачи учебной дисциплины: изучение студентами методологии проектирования и реализации системы защиты информации, с учетом угроз, характерных для современных интранет-сетей. Ставятся задачи: на лекционных занятиях познакомить студентов с основами технологий обеспечения информационной безопасности (ИБ) и рассмотреть использование этих технологий для построения систем ИБ, снижающих риски, характерные для корпоративных сетей.
Студенты, после успешного прохождения курса могут проектировать и реализовывать системы защиты интранет сетей с учетом характерных для них

угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений.

10. Место учебной дисциплины в структуре ООП: дисциплина вариативной части цикла (Б1.В). Входные знания: «Иностранный язык в профессиональной сфере».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

Компетенция		Планируемые результаты обучения
Код	Название	
ОК-7	Способность к профессиональной эксплуатации современного оборудования и приборов	знать: технологии обеспечения информационной безопасности (ИБ) в современных интранет-сетях уметь: проводить разработку и исследование моделей угроз и нарушителя ИБ объектов, в процессе планирования контрмер ИБ; владеть: способностью к профессиональной эксплуатации современного аппаратного и программного обеспечения систем информационной безопасности.
ОПК-5	Владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.	знать: типовое использование технологий обеспечения информационной безопасности для построения систем ИБ, снижающих риски, характерные для корпоративных сетей; уметь: проектировать системы защиты интранет-сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений; реализовывать системы защиты интранет-сетей; владеть: методами анализа состояния защищенности интранет-сети; средствами администрирования систем ИБ интранет-сетей;
ПК-8	Умение проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение,	знать: технологии обеспечения информационной безопасности (ИБ) в современных интранет-сетях; типовое использование этих технологий для построения систем ИБ, снижающих риски, характерные для корпоративных сетей; уметь: проектировать системы защиты интранет-сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с

	наука, техника, образование, медицина, административное управление.	использованием аппаратных решений; реализовывать системы защиты интранет-сетей; владеть: методами анализа состояния защищенности интранет-сети; средствами администрирования систем ИБ интранет-сетей;

12 Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом – 4 ЗЕТ /144 час.

Форма промежуточной аттестации *зачет с оценкой*

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)				
	Всего	Интерактив-ные часы	По семестрам		
			№ сем. 2	…..	…..
Аудиторные занятия	50	15	50		
в том числе: лекции	16		16		
Практические	-		-		
Лабораторные	34		34		
Самостоятельная работа	94		94		
Итого:	144		144		

13.1 Содержание дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности	Интранет сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности.
2	Сети IPv4, IPv6 и технология IPSec	IPSec – технология для сетей, построенных на IPv4 и IPv6.
3	Технологии виртуальных частных сетей	VPN технологии: задачи, основные типы, способы реализации.
4	RADIUS. Сетевой карантин	NAS-серверы. Централизация аутентификации на основе RADIUS. Отказоустойчивость RADIUS.
5	Инфраструктура открытых ключей. Смарт-карты.	Инфраструктура открытых ключей. Различные архитектуры доверия. Проблемы развертывания и многоуровневые PKI-решения. Многофакторная аутентификация, смарт-карты.
6	Безопасность хранения и обработки данных в ОС хостов	Безопасность хранения данных. Шифрация данных масштаба файлов, файловых систем, носителей. Безопасность ОС в корпоративной сети: шаблоны и эталоны безопасности, системы обновлений.
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	Безопасность сетевых устройств 2 уровня с ОС IOS. Безопасность сетевых устройств 3 уровня с ОС IOS. TACACS, RADIUS – решения для сетевого оборудования.
8	Аппаратная реализация IPSec, VPN.	Реализация IPSec в ОС IOS. Реализация VPN в ОС IOS.
9	Аппаратная реализация межсетевых экранов, IDS,	Обеспечение ИБ интранет сетей - как задача управления рисками. Стратегии управления рисками, технологии

	IPS.	внедрения управления рисками. Проектирование модульной инфраструктуры интранет сетей на основе типовых решений (проект CISCO SAFE).
2. Практические занятия		
3. Лабораторные работы		
2	Сети IPv4, IPv6 и технология IPSec	Создание IPSec соединения между серверами Windows с сертификационной аутентификацией
3	Технологии виртуальных частных сетей	Развертывание RAS-сервера в Windows и настройка VPN подключения с использованием PPTP.
4	RADIUS. Сетевой карантин	Установка RADIUS-сервера IAS и политик доступа для VPN-клиентов. NPS. NAP.
5	Инфраструктура открытых ключей. Смарт-карты.	Развертывание 2-уровневой PKI на компьютерах под управлением Windows Server. Создание сертификационных шаблонов для автовыпуска сертификатов. Создание субъекта, уполномоченного выпускать сертификаты для смарт-карты. Резервное копирование в PKI. Создание DRA и KRA.
6	Безопасность хранения и обработки данных в ОС хостов	Развертывание EFS. Шифрация BitLocker Drive. Применение эталонных шаблонов безопасности к серверной и клиентской ОС (Windows 2003, XP). Создание инфраструктуры WSUS в лабораторной сети.
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	Обеспечение безопасности коммутаторов с ОС IOS. Обеспечение безопасности коммутаторов 3 уровня и маршрутизаторов с ОС IOS. Настройка TACACS, RADIUS для централизованной аутентификации.
8	Аппаратная реализация IPSec, VPN.	Реализация IPSec в ОС IOS занятие 1, 2. Реализация VPN в ОС IOS с помощью SDM. Реализация VPN в ОС IOS в командном интерфейсе.
9	Аппаратная реализация межсетевых экранов, IDS, IPS.	Аппаратная реализация межсетевых экранов на основе пакетной фильтрации. Аппаратная реализация зональных межсетевых экранов на основе классификаторов трафика. Аппаратная реализация IPS (IOS).

13.2 Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности	1	-			1
2	Сети IPv4, IPv6 и технология IPSec	2	-	4	10	16
3	Технологии виртуальных частных сетей	2	-	2	8	12
4	RADIUS. Сетевой карантин	1	-	2	10	13
5	Инфраструктура открытых ключей. Смарт-карты.	2	-	6	16	24
6	Безопасность хранения и обработки данных в ОС хостов	1	-	6	12	18
7	Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения.	2		6	22	31
8	Аппаратная реализация IPSec,	2		6	8	16

	VPN.					
9	Аппаратная реализация межсетевых экранов, IDS, IPS.	3		2	8	13
	Итого:	16		34	94	144

14. Методические указания для обучающихся по освоению дисциплины

Дисциплина требует работы с файлами-презентациями лекций и соответствующими главами рекомендованной основной литературы, а также, обязательного выполнения всех лабораторных заданий в компьютерном классе. Самостоятельная подготовка к лабораторным занятиям не требуется, т.к. необходимые рекомендации даются в аудитории, где выполняются лабораторные работы.

Самостоятельная работа проводится в компьютерных классах ФКН с использованием методических материалов расположенных на учебно-методическом сервере ФКН "\\fs.cs.vsu.ru\Library" и на сервере Moodle ВГУ moodle.vsu.ru, выполнением задач конфигурирования виртуализированной ИС. Во время самостоятельной работы студенты используют электронно-библиотечные системы, доступные на портале Зональной Библиотеки ВГУ по адресу www.lib.vsu.ru. Часть заданий может быть выполнена вне аудиторий на домашнем компьютере, после копирования методических указаний и необходимого ПО с учебно-методического сервера ФКН.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	*Петренко, С.А. Аудит безопасности Intranet : учебное пособие / С.А. Петренко, А.А. Петренко. – Москва : ДМК Пресс, 2010. – 387 с. // ЭБС Лань. – URL: https://e.lanbook.com/book/1113*
2	*Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях : учебное пособие. – Москва : ДМК Пресс, 2012. – 592 с. // ЭБС Лань. – URL: https://e.lanbook.com/book/3032*
3	*Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб. : Лань, 2016. — 324 с. // ЭБС Лань. – URL: https://e.lanbook.com/book/75515*

б) дополнительная литература:

№ п/п	Источник
4	*Нестеров, С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft / С.А. Нестеров. - М. : Интернет-Университет Информационных Технологий, 2009. - 233 с. // ЭБС Лань. – URL: http://biblioclub.ru/index.php?page=book&id=234529*
5	*Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П.Н. Девянин – Москва : Горячая линия - Телеком, 2012 – 320 с. // ЭБС Университетская библиотека. – URL:http://biblioclub.ru/index.php?page=book&id=253178*
6	*Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 3-е изд., стер. - Москва : Флинта, 2011. - 224 с. // Университетская библиотека online : электронно-библиотечная система. – URL : http://biblioclub.ru/index.php?page=book&id=93351*
7	*Хабракен Д. Маршрутизаторы Cisco. Практическое применение / Д. Хабракен. – Москва: ДМК Пресс, 2008. – 316 с. // ЭБС Лань. – URL : https://e.lanbook.com/reader/book/1076*
8	*Cisco SAFE Reference Guide. – USA : Cisco Press, 2010. – 354 с. [Электронный ресурс]. URL: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf (дата обращения: 01.08.2013).*
9	*Галицкий А.В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – Москва : ДМК Пресс, 2004. - 613 с.*

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	*Библиотека ВГУ, http://www.lib.vsu.ru*
2	*Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library*
3	*Образовательный портал "Электронный университет ВГУ", http://edu.vsu.ru*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сервер учебно-методических материалов ФКН, \\fs.cs.vsu.ru\Library
2	Сервер Moodle ВГУ, http://moodle.vsu.ru

17. Информационные технологии, используемые для реализации учебного процесса по дисциплине, включая программное обеспечение и информационно-справочные системы (при необходимости)

1. Технологии виртуализации:
   Среда виртуализации Microsoft Virtual PC
   Среда виртуализации Oracle/Sun Virtual Box
   Среда виртуализации KVM/libvirt
2. Электронно-библиотечная системы «Университетская библиотека online» (http://biblioclub.ru) и «Лань» (http://lanbook.com)
3. Образовательный портал Moodle (сервер Moodle ВГУ)
4. Серверные и клиентские ОС Microsoft.
5. Операционная система GNU/Linux (дистрибутив CentOS).
6. Аппаратные сетевые экраны D-Link, CISCO.
7. АПКШ Континент IPC-25 в исполнении ЦУС и КШ компании «ООО Код Безопасности»
8. ПО Secret Net Studio компании «ООО Код Безопасности»

18. Материально-техническое обеспечение дисциплины

1. Лекционная аудитория, оснащенная видеопроектором.

2. Компьютерный класс для проведения лабораторных занятий, оснащенный программным обеспечением VirtualBox, VirtualPC. Объем свободной после загрузки ОС оперативной памяти на рабочее место не менее 4 ГБ (требуется для виртуальных машин).

3. Лаборатории программно-аппаратных средств обеспечения информационной безопасности (ауд. 303п), включающая аппаратно-программные СЗИ: смарт-карты, RFID-токены и карты, карт-ридеры; аппаратные IPS, IDS, VPN системы; развернутая виртуальная сетевая инфраструктура для выполнения лабораторных работ с аппаратными сетевыми экранами и VPN.

4. Лаборатория безопасности компьютерных сетей (ауд. 384), включающая коммутаторы и маршрутизаторы CISCO, аппаратный межсетевой экран, программный анализатор сетевого трафика WireShark. Программный симулятор, для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ.

19. Фонд оценочных средств:

19.1 Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ОК-7 Способность к профессиональной эксплуатации современного оборудования и приборов	знать: технологии обеспечения информационной безопасности (ИБ) в современных интранет-сетях	1 Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности 2 Сети IPv4, IPv6 и	Контрольная работа
	уметь: проводить разработку и исследование моделей угроз и нарушителя ИБ объектов, в процессе планирования контрмер ИБ;		Лабораторные задания №1-8

	владеть: способностью к профессиональной эксплуатации современного аппаратного и программного обеспечения систем информационной безопасности.	технология IPSec 3 Технологии виртуальных частных сетей 4 RADIUS. Сетевой карантин 5 Инфраструктура открытых ключей. Смарт-карты. 6 Безопасность хранения и обработки данных в ОС хостов 7 Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения. 8 Аппаратная реализация IPSec, VPN. 9 Аппаратная реализация межсетевых экранов, IDS, IPS.	
ОПК-5 Владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.	знать: типовое использование технологий обеспечения информационной безопасности для построения систем ИБ, снижающих риски, характерные для корпоративных сетей;	1 Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности 2 Сети IPv4, IPv6 и технология IPSec 3 Технологии виртуальных частных сетей 4 RADIUS. Сетевой карантин 5 Инфраструктура открытых ключей. Смарт-карты. 6 Безопасность хранения и обработки данных в ОС хостов 7 Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения. 8 Аппаратная реализация IPSec, VPN. 9 Аппаратная реализация межсетевых экранов, IDS, IPS.	Контрольная работа
	уметь: проектировать системы защиты интранет-сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений; реализовывать системы защиты интранет-сетей;		Лабораторные задания №1-8
	владеть: методами анализа состояния защищенности интранет-сети; средствами администрирования систем ИБ интранет-сетей;		
ПК-8 Умение проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление.	знать: технологии обеспечения информационной безопасности (ИБ) в современных интранет-сетях; типовое использование этих технологий для построения систем ИБ, снижающих риски, характерные для корпоративных сетей;	1 Интранет-сети: идентификация угроз, анализ рисков, создание системы противодействия, разработка ответных мер для возможных нарушениях безопасности 2 Сети IPv4, IPv6 и технология IPSec 3 Технологии виртуальных частных сетей 4 RADIUS. Сетевой карантин 5 Инфраструктура открытых ключей. Смарт-карты. 6 Безопасность хранения и обработки данных в ОС хостов 7 Безопасность сетевых устройств 2 и 3 уровней. TACACS, RADIUS - решения. 8 Аппаратная реализация IPSec, VPN.	Контрольная работа
	уметь: проектировать системы защиты интранет-сетей с учетом характерных для них угроз и возможностей современных технологий, как на основе ПО сетевых ОС, так и с использованием аппаратных решений; реализовывать системы защиты интранет-сетей;		Лабораторные задания №1-8
	владеть: методами анализа состояния защищенности интранет-сети; средствами администрирования систем ИБ интранет-сетей;		

		9 Аппаратная реализация межсетевых экранов, IDS, IPS.	
Промежуточная аттестация			Контрольная работа и одно лабораторное задание

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Расчет итоговой оценки описан в п. 19.4 Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом предметной области, способен иллюстрировать ответ примерами, данными научных исследований, применять теоретические знания для решения практических задач.	Повышенный уровень	Отлично
Обучающийся владеет понятийным аппаратом данной области, способен формулировать основные понятия, но затрудняется приводить примеры, характеризующие особенности предметной области	Базовый уровень	Хорошо
Обучающийся частично владеет основами дисциплины, фрагментарно способен формулировать основные понятия, но затрудняется приводить примеры и применяющиеся в них технологии	Пороговый уровень	удовлетворительно
Обучающийся демонстрирует отрывочные, фрагментарные знания не понимает основных понятий предметной области и допускает грубые ошибки.		Неудовлетворительно

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.2 Перечень практических заданий (лабораторных работ)

N	Задачи лабораторной работы
1	Создание IPSec соединения между серверами Windows с сертификационной аутентификацией
2	Развертывание RAS-сервера в Windows и настройка VPN подключения с использованием PPTP.
3	Установка RADIUS-сервера IAS и политик доступа для VPN-клиентов. NPS. NAP.
4	Развертывание 2-уровневой PKI на компьютерах под управлением Windows Server. Создание сертификационных шаблонов для автовыпуска сертификатов. Создание субъекта, уполномоченного выпускать сертификаты для смарт-карты. Резервное копирование в PKI. Создание DRA и KRA.
5	Развертывание EFS. Шифрация BitLocker Drive. Применение эталонных шаблонов безопасности к серверной и клиентской ОС (Windows 2003, XP). Создание инфраструктуры WSUS в лабораторной сети.
6	Обеспечение безопасности коммутаторов с ОС IOS. Обеспечение безопасности коммутаторов 3 уровня и маршрутизаторов с ОС IOS. Настройка TACACS, RADIUS для централизованной аутентификации.
7	Реализация IPSec в ОС IOS занятие 1, 2. Реализация VPN в ОС IOS с помощью SDM. Реализация VPN в ОС IOS в командном интерфейсе.
8	Аппаратная реализация межсетевых экранов на основе пакетной фильтрации. Аппаратная реализация зональных межсетевых экранов на основе классификаторов трафика. Аппаратная реализация IPS (IOS).

19.3.4 Перечень заданий для контрольных работ

№	Вопросы контрольной работы
1	Что такое IPsec, какие задачи решает, в чем отличие и/или несоответствие термину VPN? Как настроить IPsec, что такое фильтры, политики IPsec? Какие средства служат для отладки IPsec? Какие уже готовые политики IPsec предконфигурированы на ОС семейства Windows?
2	Опишите жизненный цикл сертификата от момента его создания. Как именно создается сертификат, в какой последовательности. Как в этом процессе участвует CA? Инструменты/утилиты для выпуска сертификатов.
3	Меры обеспечения информационной безопасности для инфраструктуры PKI.
4	Что такое удостоверяющий центр (CA – Certification Authority)? Назовите типы и роли CA. Что такое иерархия CA, что принимают во внимание при проектировании этой иерархии?
5	Что такое транспортный режим и туннельный режим IPsec? Для чего используется протокол IKE в IPsec? Для чего используются фильтры IPsec?
6	Что такое WSUS, какие задачи решает, из каких компонентов состоит? MBSA – основные режимы и возможности.
7	Для чего используются протоколы ESP AH в IPsec? Какие проблемы могут возникать у IPsec при использовании NAT?
8	Что такое VPN, перечислите компоненты VPN. Какие существуют технологии реализации VPN, какие требования к IP-сети предъявляет каждая технология?
9	Для чего используется протокол IKE в IPsec? Что такое SA, main-mode (основной режим) quick-mode (оперативный режим)? Какие три вида аутентификации конечных систем обычно поддерживаются в реализациях IPsec? Когда какой используется?
10	Что такое сетевой экран уровня «приложения», в чем отличие от сетевого экрана «пакетный фильтр»? Что такое unsolicited трафик и чем отличаются файерволы statefull и stateless? Как размещены по отношению к корпоративной сети сетевые экраны, опишите основные архитектуры
11	Что такое EFS, какие задачи решает, из каких компонентов состоит? Как технически реализована возможность расшифровки файла другими пользователями, перечислите условия, в которых это возможно?

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущих и промежуточной аттестаций. Текущие аттестации проводятся в форме письменной контрольной работы с вопросами по лекционной части курса и лабораторных заданий, позволяющих оценить степень сформированности умений и навыков. Промежуточная аттестация проводится в форме: письменной работы. При оценивании контрольных и лабораторных работ используется количественная шкала оценок.

При оценивании за каждый вопрос письменной контрольной работы или действие лабораторной работы устанавливается балльная оценка: 0 – не выполнено/нет ответа/выполнено неверно; 1 – частично выполнено/не полный ответ/отчасти верно; 2 – полностью выполнено/полностью верно. Итоговая оценка формируется суммированием и нормированием к 50-балльной оценке раздельно для каждого текущего или промежуточного оценивания. Итоговая оценка за предмет (оценка промежуточной аттестации) устанавливается согласно положению о балльно-рейтинговой системе факультета компьютерных наук (на основе оценок промежуточной и текущих аттестаций). В частности используется следующая шкала:

оценка «отлично» - 90..100 баллов
оценка «хорошо» - 70..89 баллов
оценка «удовлетворительно» - 50..69 баллов
оценка «неудовлетворительно» - 0..49 баллов.

Кроме того, условием положительной оценки является выполнение на занятиях и сдача преподавателю результатов всех лабораторных работ курса.

Оценочные средства промежуточной и текущих аттестаций размещены на файл-сервере ФКН по адресу "\\fs.cs.vsu.ru\Library\Лекции" и на сервере Moodle ВГУ moodle.vsu.ru.