МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет химии и высоких технологий

УТВЕРЖДАЮ:
Проректор по учебной работе, качеству образования – первый проректор
_____Хагуров Т.А.
«31» ____мая_____ 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ФТД.03 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки – 04.03.01 Химия

Направленность (профиль) – «Аналитическая химия»

Форма обучения – очная

Квалификация выпускника – бакалавр

Краснодар 2024

Рабочая программа дисциплины ФТД.03 «Информационная безопасность» составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 04.03.01 – Химия.

Программу составил:

Волынкин В.А., зав. кафедрой общей, неорганической химии и информационно-вычислительных технологий в химии, к.х.н., доцент _____

Рабочая программа дисциплины ФТД.03 «Информационная безопасность» утверждена на заседании кафедры общей, неорганической химии и ИВТ в химии
протокол № 8 от «23» апреля 2024 г.

Заведующий кафедрой Волынкин В.А. _____

Утверждена на заседании учебно-методической комиссии факультета химии и высоких технологий, протокол № 7 «20» мая 2024 г.

Председатель УМК факультета Беспалов А.В. _____

Рецензенты:

Крапивин Г.Д, главный научный сотрудник ЦКП «ИЦПиХТ»
ФГБОУ ВО «КубГТУ», д.х.н., профессор

Болотин С.Н, зав. кафедрой экологии и природопользования
ФГБОУ ВО «КубГУ», к.х.н, доцент

1. Цели и задачи освоения дисциплины

1.1. Цель освоения дисциплины:

Формирование у студентов системы знаний об основах защиты информации в локальной и глобальной сети и основах защиты баз данных.

Формирование представлений об основных векторах программных, криптографических и социально-инженерных атак; эффективных методах и приемах информационной защиты.

1.2. Задачи дисциплины:

- овладение приемами и стандартными практиками защиты информации;
- формирование эффективных навыков информационной защиты личной, служебной и ведомственной информации;
- формирование умений по использованию базовых программных средств и практик защиты личных, служебных и ведомственных информационных ресурсов;
- изучение номенклатуры технологических решений, служебных протоколов и имеющихся методов информационной защиты.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Курс «Информационная безопасность» относится к факультативным дисциплинам (ФТД.03). В соответствии с рабочим учебным планом дисциплина изучается на третьем курсе по очной форме обучения. Вид промежуточной аттестации: зачет. Для его изучения используются знания школьного общеобразовательного курса «Информатика». Знания и навыки, полученные в результате освоения данного курса, могут быть использованы при изучении большинства дисциплин, таких как неорганическая химия, аналитическая химия, физическая химия, строение вещества, химическая технология и других, в научно-исследовательской работе студентов.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ОПК-5. Способен использовать существующие программные продукты и информационные базы данных для решения задач профессиональной деятельности с учетом основных требований информационной безопасности.	
ИОПК-5.2. Использует современные IT-технологии при сборе, анализе, обработке и представлении информации химического профиля ИОПК-5.3. Соблюдает нормы информационной безопасности в профессиональной деятельности	Знает теоретические основы создания документов для обработки данных, выполнения расчетов и представления результатов выполненных работ
	Умеет создавать документы для обработки данных, выполнения расчетов и представления результатов выполненных работ
	Владеет программным обеспечением для работы с деловой и научной информацией и основами Интернет технологий

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			5			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**34**	**34**			
Занятия лекционного типа		16	18		-	-
Лабораторные занятия		18	18		-	-
Занятия семинарского типа (семинары, практические занятия)					-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)						
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**37,8**	**37,8**			
Курсовая работа		-	-		-	-
Проработка учебного (теоретического) материала		12	12		-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		6	6		-	-
Реферат		6	6		-	-
Подготовка к текущему контролю		13,8	13,8			
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**72**	**72**		**-**	**-**
	в том числе контактная работа	**70,2**	**70,2**			
	зач. ед	**2**	**2**			

2.2 Содержание дисциплины.

Распределение видов учебной работы и их трудоёмкости по разделам дисциплины. Разделы дисциплины, изучаемые в 5 семестре (для студентов ОФО).

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Основные понятия защитыинформации и информационной безопасности	8	4			4
2.	Политика и стандарты информационной безопасности	8	4		2	4
3.	Принципы криптографической защиты информации	18	6		6	6
4.	Технологии защиты межсетевого обмена данными	8	4			4
5.	Основы технологии виртуальных защищенныхсетей	14	4		4	6
6.	Технологии обнаружения вторжений	31,8	12		6	13,8
	ИТОГО по разделам дисциплины	71,8	16		18	37,8
	Контроль самостоятельной работы (КСР)					
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Основные понятия защитыинформации и информационной безопасности	Базовые понятия и основы информационной безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Введение в сетевой информационный обмен. Анализ угроз информационной безопасности. Обеспечение информационной безопасности сетей. Угрозы и уязвимости беспроводных сетей.	*К*
2.	Политика и стандарты информационной	Основные понятия политики безопасности. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Про-	*Р*

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
	безопасности	цедуры безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий.	
3.	Принципы криптографической защиты информации	Основные понятия криптографической защиты информации. Симметричные, асимметричные и комбинированная криптосистемы шифрования. Электронная цифровая подпись и функция хэширования. Управление криптоключами. Криптографические алгоритмы и их классификации. Блочные алгоритмы шифрования данных. Алгоритм шифрования RSA. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификацияпользователя.	*Т*
4.	Технологии защиты межсетевого обмена данными	Обеспечение безопасности операционных систем (ОС). Проблемы обеспечения безопасности ОС. Угрозы безопасности. Архитектура подсистемызащиты ОС. Основные функции подсистемы защиты ОС. Идентификация, аутентификация и авторизация субъектов доступа. Функции межсетевых экранов (МЭ). Особенности функционирования МЭ на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ. Формирование политики межсетевого взаимодействия. Персональные и распределительные сетевые экраны. Проблемы безопасности МЭ.	*Проверка выполнения работ. Отчеты о выполнении.*
5.	Основы технологии виртуальных защищенных сетей	Концепция построения виртуальных защищенных сетей VPN. Основные понятия и функции сети VPN. Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN. Достоинства применения технологий VPN. Протоколы формирования защищенных каналов на канальном уровне (PPTP и L2TP). Протоколы формирования защищенных каналов на сеансовом уровне (SSL/TLS и SOCKS). Защита на сетевом уровне – протокол IPSEC. Инфраструктура защиты на прикладном уровне. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией SingleSign-On (SSO). Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.	*Р*

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
6.	Технологии обнаружения вторжений	Анализ защищенности и обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Технологии обнаружения атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Методы реагирования. Защита от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети.	*Коллоквиум с докладами в виде презентации*

2.3.2 Занятия семинарского типа

Планом не предусмотрены

2.3.3 Лабораторные занятия

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1.	Проводник. Основные понятия ФС. Работа с командной строкой.	*Отчет по лаб. работе*
2.	Системы счисления. Особенности работы с числами в разных системах счисления.	*Решение задач*
3.	Microsoft Word. Шрифт, абзац, разметка страницы.	*Отчет по лаб. работе*
4.	Microsoft Word. Структура документа, использование стилей.	*Отчет по лаб. работе*
5.	Microsoft Word. Работа с таблицами. Формулы, рисунки.	*Отчет по лаб. работе*
6.	Microsoft Excel. Построение диаграмм.	*Отчет по лаб. работе*
7.	Microsoft Excel. Обработка данных методом наименьших квадратов.	*Отчет по лаб. работе*
8.	Microsoft Excel. Построение диаграмм, решение уравнений.	*Отчет по лаб. работе*
9.	Работа с ChemSketch. Создание химических формул, схем и т.д.	*Отчет по лаб. работе*

2.3.4 Примерная тематика курсовых работ

Курсовые работы – не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Теоретическая самоподготовка	Методические рекомендации к организации аудиторной и внеаудиторной (самостоятельной) работы студентов: методические указания / сост. Т.П. Стороженко, Т.Б. Починок, А.В. Беспалов, Н.В. Лоза. – Краснодар: Кубанский гос. ун-т, 2018. 89 с. Информатика: программирование и численные методы: лабораторный практикум / [сост. В. А. Волынкин, И. В. Сухно, В. Ю. Бузько]; Кубанский гос. ун-т. – Краснодар, 2010. - 75 с. Интернет ресурсы по дисциплине, в том числе указанные в п.6.
2	Подготовка к ЛР	
3	Реферат	
4	Доклады, презентации	

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

Для формирования профессиональных компетенций в процессе освоения курса используется технология профессионально-развивающего обучения, предусматривающая не только передачу теоретического материала, но и стимулирование и развитие продуктивных познавательных действий студентов (на основе психолого-педагогической теории поэтапного формирования умственных действий).

Активизации и интенсификации познавательного процесса способствуют моделирование проблемных ситуаций, мультимедийные презентации в лекционном курсе. В рамках лабораторных занятий применяются методы проектного обучения, исследовательские методы, тренинговые формы, метод

конкретных ситуаций. В процессе самостоятельной деятельности студенты осваивают и анализируют передовой опыт, используя имеющуюся литературу и информационные технологии, выступают с презентациями, накапливают портфолио разработок.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационно-коммуникационные технологии и анализ данных». Оценочные средства включают контрольные материалы для проведения текущего контроля в форме тестовых заданий, доклада-презентации по проблемным вопросам, контрольных работ и промежуточной аттестации в форме вопросов к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИОПК-5.2. Использует современные IT-технологии при сборе, анализе, обработке и представлении информации химического профиля	Умеет создавать документы для обработки данных, выполнения расчетов и представления результатов выполненных работ	Лабораторные работы, Расчетные кейс задания	Вопросы на зачете 1, 11 - 14
2	ИОПК-5.3. Соблюдает нормы информационной безопасности в профессиональной деятельности	Владеет программным обеспечением для работы с деловой и научной информацией и основами Интернет технологий	Реферат, доклад-презентация, вопросы для устного опроса.	Вопросы на зачете 22-24

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

Примерные темы рефератов, докладов, эссе

1. Закон об информации, информационных технологиях и о защите информации.
2. Закон о безопасности критической информационной инфраструктуры Российской Федерации.
3. Закон о связи и информационная безопасность.
4. Виды и функции электронной подписи.

5. Защита персональных данных.
6. Социально-инжиниринговые атаки, их виды. Примеры социально-инжиниринговых атак.
7. Фишинг и целевой фишинг.
8. Сетевые атаки.
9. Программы-прослушиватели сетевых протоколов. Сканирование сетевых портов. Сетевые сканеры.
10. Атаки вида «отказ в обслуживании».
11. Атаки, использующие уязвимости программных средств.
12. Уязвимость «переполнение стека».
13. VPN-соединения.
14. Атаки, использующие скриптовые вставки в интерпретирующие программные среды.
15. Атака SQL-insertion.
16. «Санация» пользовательского ввода.
17. Атака «подмены источника».
18. Криптографические атаки.
19. Классические шифры: шифр Цезаря, Виженера, Кардано.
20. Шифровальные блокноты.
21. Устаревшие и актуальные шифры. DES-шифрование.
22. Понятие «односторонней» функции.
23. Симметричные системы шифрования. Асимметричные системы шифрования.
24. Электронная цифровая подпись.
25. Хэш-функции.
26. Управление криптографическими ключами.
27. Стеганографические методы шифрования данных.
28. Атаки, использующие словари паролей.
29. Атаки, использующие уязвимости операционных систем.
30. Уязвимости Meltdown и Spectre.
31. Профилактика социально-инжиниринговых атак.
32. Профилактика криптографических атак.
33. Профилактика атак, использующих уязвимости программных сред.
34. Профилактика атак на сетевую инфраструктуру.
35. Профилактика атак на операционные системы.
36. Прямые и косвенные признаки программно-вирусного заражения.
37. Виды вирусных атак. Вирусы «трояны». Запись с клавиатуры (key-logging). Вирусы шифровальщики.
38. Профилактика программно-вирусных заражений.
39. Нетрадиционные методы несанкционированного доступа.
40. Организация доступа в современных операционных системах.
41. Обеспечение безопасности операционных систем. Задачи системного администрирования.

42. Управление политикой безопасности. Разграничение доступа. Изоляция программ. Изоляция среды исполнения.
43. Виртуализация операционных систем. Виртуальные среды исполнения (контейнеры).

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

Вопросы для подготовки к зачету

1. Эволюция каналов передачи информации.
2. Понятия и определения области информационной безопасности.
3. Информационные угрозы и способы защиты от них.
4. Доктрина информационной безопасности РФ.
5. Законодательный уровень защиты информации.
6. Процедурный уровень обеспечения информационной безопасности.
7. Компьютерные вирусы и антивирусные программы. 8.Методы и технологии борьбы с компьютерными вирусами. 9.Криптография.
10. Биометрия.
11. Индивидуальная и государственная защита информации.
12. Информационная война.
13. Особенности управления информацией в городах.
14. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.
15. Информационная экономика.
16. Глобальная информатизация общества.
17. Реклама как источник информационной опасности.
18. Информационные образовательные технологии XXI века.
19. Географические информационные системы.
20. Априорный анализ надежности.

Критерии оценивания результатов обучения

Оценки «зачет» заслуживает студент, обнаруживший сформированность компетенций, предусмотренных программой дисциплины, необходимых для дальнейшей учёбы и предстоящей работы по профессии, справляющийся с выполнением заданий, предусмотренных программой.

Оценка «незачет» выставляется студенту, обнаружившему значительные пробелы в знаниях основного программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка «незачет» ставится студентам, которые не освоили в должной мере функции преподавателя химии и не смогут приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующим дисциплинам.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Учебная литература

1. Информатика. Базовый курс [Текст] : учебное пособие для студентов втузов / под ред. С. В. Симоновича. - 3-е изд. - Санкт-Петербург [и др.] : Питер, 2018. - 637 с.
2. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — Саратов: Вузовское образование, 2019. — 214 с.
3. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов : Ай Пи Эр Медиа, 2019. — 227 с.
4. Чернова Е. В. Информационная безопасность человека : учебное пособие для вузов /

5. Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с.
6. Шаньгин В.Ф. Информационная безопасность и защита информации: учеб. пособие / В.Ф. Шаньгин.- Саратов:Профобразование, 2017.- 702с.

5.2. Периодическая литература

Указываются печатные периодические издания из «Перечня печатных периодических изданий, хранящихся в фонде Научной библиотеки КубГУ» https://www.kubsu.ru/ru/node/15554, *и/или электронные периодические издания, с указанием адреса сайта электронной версии журнала, из баз данных, доступ к которым имеет КубГУ:*

1. Базы данных компании «Ист Вью» http://dlib.eastview.com
2. Журнал «Информатизация и связь»
3. Журнал «Инфокоммуникационные технологии»
4. Журнал «Программные продукты и системы»
5. Журнал «Прикладная информатика»

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
2. ЭБС «ZNANIUM.COM» www.znanium.com
3. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Scopus http://www.scopus.com/
2. ScienceDirect www.sciencedirect.com
3. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
4. zbMath https://zbmath.org/
5. "Лекториум ТВ" http://www.lektorium.tv/

Ресурсы свободного доступа:

1. http://www.ixbt.com
2. http://www.alleng.ru/edu/comp.htm
3. http://www.computer-museum.ru
4. https://compress.ru/
5. https://www.computerra.ru/
6. https://www.osp.ru/pcworld
7. Федеральный портал "Российское образование" http://www.edu.ru/;
8. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;

9. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
10. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

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

В.А. Волынкин, И.В. Сухно, В.Ю. Бузько. Информатика. Программирование и численные методы. Лабораторный практикум. Краснодар, КубГУ, 2010, 76 с.

Методические рекомендации преподавателям по методике проведения основных видов учебных занятий

Лекции

Методика чтения лекций

Лекции являются одним из основных методов обучения по дисциплине, которые должны решать следующие задачи:

- изложить важнейший материал программы курса, освещающий основные моменты;
- развить у студентов потребность к самостоятельной работе над учебной и научной литературой.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее главных положений. Рекомендуется на первой лекции довести до внимания студентов структуру курса и его разделы, а в дальнейшем указывать начало каждого раздела, суть и его задачи, а, закончив изложение, подводить итог по этому разделу, чтобы связать его со следующим.

Содержание лекций

Содержание лекций определяется рабочей программой курса. Крайне желательно, чтобы каждая лекция охватывала и исчерпывала определенную тему курса и представляла собой логически вполне законченную работу.

Лучше сократить тему, но не допускать перерыва ее в таком месте, когда основная идея еще полностью не раскрыта.

Лабораторные занятия

Методика проведения лабораторных занятий

Целями проведения лабораторных работ являются:

- установление связей теории с практикой в форме экспериментального подтверждения положений теории;
- обучение студентов умению анализировать полученные результаты;
- контроль самостоятельной работы студентов по освоению курса;
- обучение навыкам профессиональной деятельности

Цели лабораторного практикума достигаются наилучшим образом в том случае, если выполнению эксперимента предшествует определенная подготовительная внеаудиторная работа. Поэтому преподаватель обязан довести до всех студентов график выполнения лабораторных работ с тем, чтобы они могли заниматься целенаправленной домашней подготовкой.

Перед началом очередного занятия преподаватель должен удостовериться в готовности студентов к выполнению лабораторной работы путем короткого собеседования и проверки наличия у студентов заготовленных протоколов проведения работы.

Указания по самостоятельной работе.

Самостоятельная работа составляет не менее 50% от времени, отводимого на изучение дисциплины. При самостоятельной работе студент должен ознакомиться с основными учебниками и учебными пособиями, дополнительной литературой и иными доступными литературными источниками. При работе с литературой по конкретным темам курса, в том числе указанным для самостоятельной проработки, основное внимание следует уделять важнейшим понятиям, терминам, определениям, для скорейшего усвоения которых целесообразно вести краткий конспект.

7. Материально-техническое обеспечение по дисциплине (модулю)

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: интерактивная доска SMART Board, короткофокусный интерактивный проектор, ноутбук, меловая доска (ауд. 234С).	Microsoft Windows, Microsoft PowerPoint
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных кон-	Мебель: учебная мебель Технические средства обучения: интерактивная доска SMART Board, короткофокусный интерактивный проектор, ноутбук, меловая доска (ауд. 234С).	Microsoft Windows, Microsoft PowerPoint

сультаций, текущего контроля и промежуточной аттестации		
Учебные аудитории для проведения лабораторных работ. Компьютерные классы.	Мебель: учебная мебель Технические средства обучения: терминальные станции с операционной системой Windows и необходимым программным обеспечением (ауд. 103).	Microsoft Windows, Microsoft Office (Word, Excel, PowerPoint), ACD Labs Chemsketch freeware, Free Pascal
Учебные аудитории для курсового проектирования (выполнения курсовых работ)	Мебель: учебная мебель Технические средства обучения: компьютерная техника с возможностью подключения к сети «Интернет» и доступом в электронную информационно-образовательную среду университета (проводное соединение и беспроводное соединение по технологии Wi-Fi). (ауд. 428с, 431с)	Microsoft Windows, Microsoft Office (Word, Excel, PowerPoint), ACD Labs Chemsketch freeware, Free Pascal