МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»
Первый проректор
И.Г.Гайрабеков
«01» 09 2021г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита информации»

Направление подготовки

09.03.01 *Информатика и вычислительная техника*

Направленность (профиль)

«Информатика и вычислительная техника»

Квалификация

Бакалавр

Год начало подготовки - 2021

Грозный - 2021

1. Цели и задачи дисциплины

Целью изучения дисциплины является ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которыми подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программам; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации.

Задача дисциплины: ознакомить студентов с тенденциями развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а также с нормативными документами и методами защиты компьютерной информации.

Место дисциплины в структуре образовательной программы

Учебная дисциплина «Защита информации» относится к Блоку 1 части, формируемой участниками образовательных отношений учебного плана. Для изучения курса требуется освоение следующих дисциплин: «Информатика», «Информационные технологии», «Теоретические основы информатики.

В свою очередь, данный курс, помимо самостоятельного значения, является дисциплиной, завершающей учебный курс, предшествующей дипломному проектированию.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код по ОП	**Индикаторы достижения**	**Планируемые результаты обучения по дисциплине (ЗУВ)**
Универсальная		
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;	**ОПК-2.1** Выбирает современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности. **ОПК – 2.2** Применяет современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.	**знать:** - содержание основных понятий обеспечения информационной безопасности, источники угроз безопасности информации, методы оценки уязвимости информации **уметь:** - разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации **владеть:** - навыками освоения и внедрения средств защиты

ОПК-3.Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.1**Формулирует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **ОПК-3.2** Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасност**и. ОПК-3.3** Демонстрирует навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	**знать**: виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты; **уметь**: выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС; **владеть**: навыками работы с различными источниками информации;

4. Объем дисциплины и виды учебной работы

Таблица 1

Вид учебной работы	**Всего часов/ зач.ед.**		**ОФО**	**ЗФО**
	ОФО	ЗФО	5 сем.	5 сем.
Контактная работа	**51/1,4**	**8/0,2**	**51/1,4**	**8/0,2**
В том числе:				
Лекции	17/0,5	2/0,1	17/0,5	2/0,1
Лабораторные работы (ЛР)	34/0,9	6/0,2	34/0,9	6/0,2
Самостоятельная работа (всего)	**57/1,6**	**100/2,7**	**57/1,8**	**96/2,7**
В том числе:				
Расчетно-графические работы				
Темы для самостоятельного изучения	20/0,5	25/0,7	20/0,5	25/0,7
Подготовка презентаций	20/0,5	50/1,4	20/0,5	50/1,4
И(или) другие виды самостоятельной работы:				

Подготовка к лабораторным работам	-	-	-	-
Подготовка к зачету	17/0,5	25/0,7	17/0,5	25/0,7
Подготовка к экзамену				
Вид отчетности	зач	зач	зач.	зач.
Общая трудоемкость дисциплины Час. Зач. ед.	108 3	108 3	108 3	108 3

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 2

№ п/п	Наименование раздела дисциплины	Лекц.		Лаб. зан.		Всего часов/з.е.	
		ОФО	ЗФО	ОФО	ЗФО	ОФО	ЗФО
5 семестр							
1	Основные понятия защиты информации и информационной безопасности	6	-	10	2	16/0,5	2/0,1
2	Структура политики безопасности организации	8	2	10	2	18/0,5	4/0,1
3	Основные понятия криптографической защиты информации	3	-	10	2	13/0,4	4/0,1

5.2. Лекционные занятия

Таблица 3

№ п/п	Наименование раздела дисциплины	Содержание раздела
5 семестр		
1.	Основные понятия защиты информации и информационной безопасности	Защита информации. Эффективность защиты информации. Защита информации от НСД. Система защиты информации. Санкционированный доступ к информации.
2.	Структура политики безопасности организации	Обзор политики безопасности. Базовая политика безопасности. Процедуры безопасности
3.	Основные понятия криптографической защиты информации	Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования.

5.3. Лабораторный практикум

Таблица 4

№ п/п	Наименование раздела	Наименование лабораторных работ
3 семестр		

1.	Основные понятия защиты информации и информационной безопасности	**Лабораторная работа № 1** Защита информации с использованием методов шифрования. **Лабораторная работа №** 2 Нормативно правовая защита информации
2.	Структура политики безопасности организации	**Лабораторная работа №3** Локальные акты по защите информации по персональным данным **Лабораторная работа №5** Компьютерная вирусология
3.	Основные понятия криптографической защиты информации	**Лабораторная работа № 6** Компьютерная криптография

5.4. Практические занятия (семинары) – не предусмотрены.

6. Самостоятельная работа

6.1. Тематика и формы самостоятельной работы студентов

5 семестр

Таблица 5

№№ п/п	Тематика докладов с презентациями
1	ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»
2	ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности»
3	ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3
4	ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
5	ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»
6	ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
7	ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»
8	ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности»
9	ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»
10	ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации»
11	Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
12	Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
13	Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
14	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.

15	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
16	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями руководящих документов Гостехкомиссии РФ.
17	Оценка защищенности компьютерной системы университета на основе ОС Windows ME (98) в соответствии с требованиями «Оранжевой книги».
18	Оценка защищенности компьютерной системы университета на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
19	Оценка защищенности компьютерной системы университета на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
20	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows ME(98) в соответствии с требованиями «Оранжевой книги».
21	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Windows XP Professional (NT, 2000) в соответствии с требованиями «Оранжевой книги».
22	Оценка защищенности компьютерной системы офиса коммерческой организации на основе ОС Linux в соответствии с требованиями «Оранжевой книги».
23	Оценка защищенности ОС Windows XP Professional (NT, 2000) в соответствии со стандартами ISO.
24	Оценка защищенности ОС Linux в соответствии со стандартами ISO.
25	Сравнительный анализ антивирусных пакетов.

Учебно-методическое обеспечение для самостоятельной работы студентов:

1.Алексеев В.А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / Алексеев В.А.. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2019. — 16 с. — ISBN 2227-8397.— Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL:http://www.iprbookshop.ru/17710.htm

2. Джонс К.Д. Инструментальные средства обеспечения безопасности : учебное пособие / Джонс К.Д., Шема М., Джонсон Б.С.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/102011.html

7. Оценочные средства

7.1. Вопросы к рубежным аттестациям

Первый семестр

Вопросы к 1ой рубежной аттестации:

1.Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности

13. Процедуры безопасности

Образец билета к1-ой рубежной аттестации:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский Государственный Нефтяной Технический Университет им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Информатика»

1-я рубежная аттестация

Вариант 1

1. Признаки классификации угроз
2. НСД к информации. Способы получения НСД

Преподаватель_____ _____ М.З.Исаева

Вопросы ко 2ой рубежной аттестации:

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования
4. Электронная цифровая подпись и функция хэширования
5. Аутентификация, авторизация и администрирование действий пользователей
6. Аутентификация на основе паролей
7. Угрозы безопасности ОС
8. Понятие защищенной ОС
9. Основные функции подсистемы защиты ОС
10. Разграничение доступа к объектам ОС
11. Аудит
12. Технология межсетевых экранов
13. Функции МЭ
14. Дополнительные возможности МЭ
15. Проблемы безопасности МЭ..

Образец билета к 2-ой рубежной аттестации:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский Государственный Нефтяной Технический Университет им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Информатика»

2-я рубежная аттестация

Вариант 1

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования

Преподаватель_____ _____ М.З. Исаева

7.2. Вопросы к зачету (1 семестр)

Основные понятия защиты информации и информационной безопасности

2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности
13. Процедуры безопасности
14. Основные понятия криптографической защиты информации
15. Симметричные криптосистемы шифрования
16. Ассиметричные криптосистемы шифрования
17. Электронная цифровая подпись и функция хэширования
18. Аутентификация, авторизация и администрирование действий пользователей
19. Аутентификация на основе многоразовых паролей
20. Аутентификация на основе одноразовых паролей
21. Аутентификация на основе PIN-кода
22. Угрозы безопасности ОС
23. Понятие защищенной ОС
24. Основные функции подсистемы защиты ОС
25. Разграничение доступа к объектам ОС
26. Аудит
27. Технология межсетевых экранов
28. Функции МЭ
29. Дополнительные возможности МЭ

Образец билета к зачету:

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова
Кафедра «ИВТ»
Дисциплина «Информатика»
Группа: **Семестр:**

Билет 1
1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования

Преподаватель _____ **М.З. Исаева**
Зав.кафедрой _____ **Э.Д.Алисултанова**

7.3. Текущий контроль

Образец типового задания для лабораторных занятий
Лабораторная работа № 1 Разграничение прав пользователей.

Задания к работе

Цель: освоение основ криптографической защиты информации.

Задачи: ознакомление с методами шифрования, использование методов шифрования, дешифрования, освоение основных понятий.

Шифрова́ние — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма. пользователи являются авторизованными, если они обладают определённым аутентичным ключом. вся сложность и, собственно, задача шифрования состоит в том, как именно реализован этот процесс. в целом,

шифрование состоит из двух составляющих — зашифровывание и расшифровывание(дешифрование).

Кодирование информации — процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки.

В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ. отсюда название — симметричные. алгоритм и ключ выбирается заранее и известен обеим сторонам. сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи. в связи с этим, возникает проблема начальной передачи ключа (синхронизации ключей). кроме того существуют методы крипто атак, позволяющие так или иначе дешифровать информацию не имея ключа или же с помощью его перехвата на этапе согласования. в целом эти моменты являются проблемой криптостойкости конкретного алгоритма шифрования и являются аргументом при выборе конкретного алгоритма.

асимметричное шифрование

В системах с открытым ключом используются два ключа — открытый и закрытый, связанные определённым математическим образом друг с другом. Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для шифрования сообщения и для проверки ЭЦП. Для расшифровки сообщения и для генерации ЭЦП используется секретный ключ.

Данная схема решает проблему симметричных схем, связанную с начальной передачей ключа другой стороне. Если в симметричных схемах злоумышленник перехватит

ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом решается проблема симметричных систем, связанная с синхронизацией ключей.

Деятельность в области криптографии (шифрования) ограничена как при ее осуществлении на территории России, так и при ввозе и вывозе криптографических (шифровальных) средств. Регулирование деятельности в области криптографии на территории России осуществляется российскими нормативными правовыми актами, ввоз и вывоз криптографических средств регламентируется актами Евразийской экономической комиссии.

Органом, осуществляющим регулирование и контроль в сфере криптографии, является Федеральная служба безопасности (ФСБ России). Она вправе:

- осуществлять в соответствии со своей компетенцией регулирование в области разработки, производства, реализации, эксплуатации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, расположенных на территории Российской Федерации, а также в области предоставления услуг по шифрованию информации в Российской Федерации, выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;
- осуществлять государственный контроль за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу информации с использованием шифров, контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также в соответствии со своей компетенцией контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;
- разрабатывать, создавать и эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации, включая средства криптографической защиты.

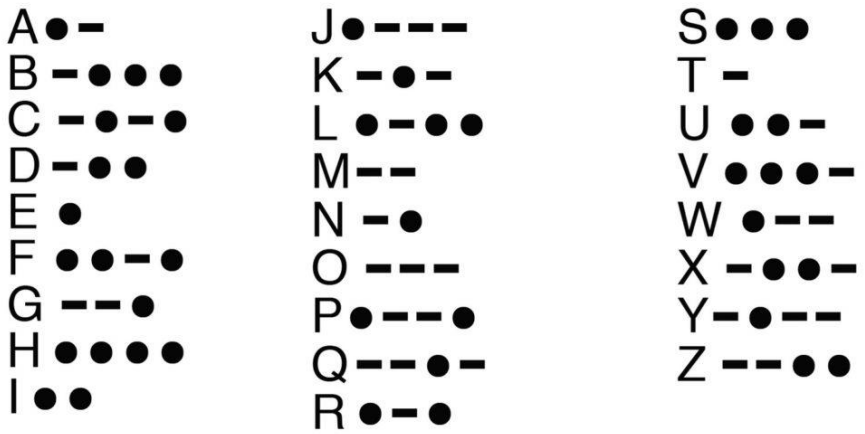
Основной документ, регулирующий отношения, касающиеся шифрования - Приказ ФСБ РФ от 9 февраля 2005 г. "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"

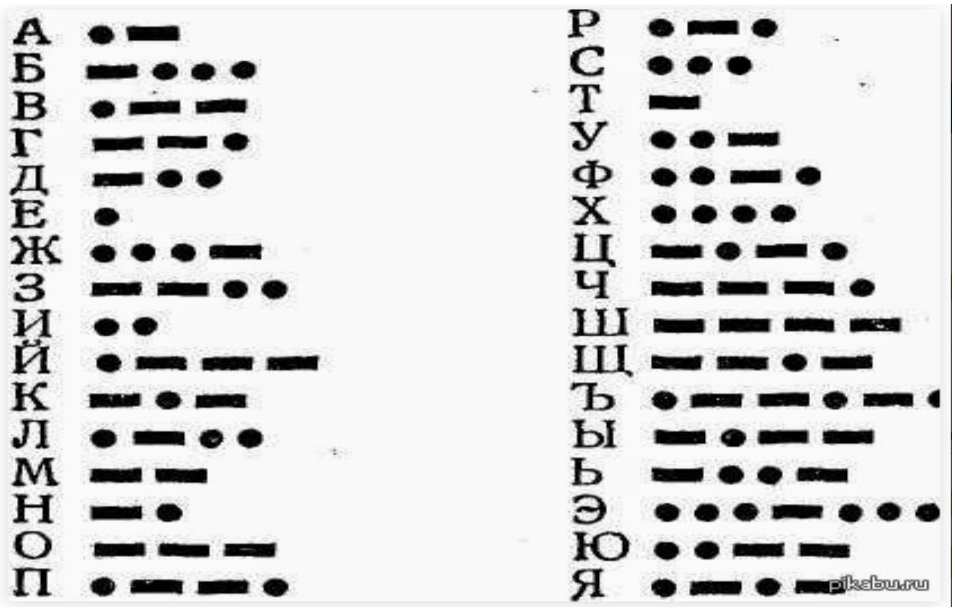
Методы шифрования. Ниже представлены некоторые методы шифрования. 1.Стеганография — это искусство скрытого письма. Этой технике даже больше лет, чем кодам и шифрованию. Например, сообщение может быть написано на бумаге, покрыто ваксой и проглочено с той целью, чтобы незаметно доставить его получателю. Другой способ — нанести сообщение на бритую голову курьера, подождать, пока волосы вырастут заново и скроют послание. Лучше всего для стеганографии использовать повседневные объекты. Когда-то в Англии использовался такой метод: под некоторыми буквами на первой странице газеты стояли крохотные точки, почти невидимые невооруженным глазом. Если читать только помеченные буквы, то получится секретное сообщение! Некоторые писали сообщение первыми буквами составляющих его слов или использовали невидимые чернила. Была распространена практика уменьшения целых страниц текста до размера буквально одного пикселя, так что их было легко пропустить при чтении чего-то относительно безобидного. Стеганографию лучше всего использовать в сочетании с другими методами шифрования, так как всегда есть шанс, что ваше скрытое послание обнаружат и прочитают.

2.ROT1. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, A заменяется на B, B на C, и т.д. «ROT1» значит «ROTate 1 letter forward through the alphabet» (англ. «сдвиньте алфавит на одну букву вперед»). Сообщение «I know what you did last summer» станет «J lopx xibu zpv eje mbtu tvnnfs». Этот шифр весело использовать, потому что его легко понять и применять, но его так же легко и расшифровать. Из-за этого его нельзя использовать для серьезных нужд, но дети с радостью «играют» с его помощью. Задание: расшифровать следующее сообщение «mpoepo jt b dbqjubm»

3.Транспозиция. В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Например, если каждое слово пишется задом наперед, то из «all the better to see you with» получается «lla eht retteb ot ees joy htiw». Другой пример — менять местами каждые две буквы. Таким образом, предыдущее сообщение станет «la tl eh eb tt re ot es ye uo iw ht». Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, чтобы посылать важные сообщения. Сложные ключи могут сделать такой шифр довольно сложным на первый взгляд, но многие сообщения, закодированные подобным образом, могут быть расшифрованы простым перебором ключей на компьютере. Расшифровать: Лэ ме не ат рн о аВстно

4.Азбука Морзе. В азбуке Морзе каждая буква алфавита, все цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов, часто называемых «точками и тире». Так, А — это «•–», В — «–•••», и т.д. В отличие от большинства шифров, азбука Морзе используется не для затруднения чтения сообщений, а наоборот, для облегчения их передачи (с помощью телеграфа). Длинные и короткие сигналы посылаются с помощью включения и выключения электрического тока.





Расшифровать: .-. .- --.. --. .- -.. -.- .-

5.Шифр Цезаря, также известный как **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее. Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить

формулами модульной арифметики[1][2]: y=(x+k) mod n x=(y-k) mod nгде x— символ открытого текста, y — символ шифрованного текста, n— мощность алфавита, а k — ключ. Пример: Шифрование с использованием ключа . Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее: Исходный алфавит: А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифрованный: Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

6.Шифр Виженера (фр. *Chiffre de Vigenère*) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.[1]

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал название **le chiffre indéchiffrable** (с французского 'неразгаданный шифр'). Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Квадрат Виженера (рис1)

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера (рис1). Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет такой вид:

```
ATTACKATDAWN
```

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

```
LEMONLEMONLE
```

Первый символ исходного текста ("A") зашифрован последовательностью L, которая является первым символом ключа. Первый символ зашифрованного текста ("L") находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ зашифрованного текста ("X") получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

```
Исходный текст:       ATTACKATDAWN
Ключ:                 LEMONLEMONLE
Зашифрованный текст:  LXFOPVEFRNHR
```

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если n — количество букв в алфавите, Mj — буквы открытого текста, Kj— буквы ключа, то шифрование Виженера можно записать следующим образом:

Cj=(Mj=Kj) mod n

И расшифровывание:

Mj=(Cj+N-Kj) mod n

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять чаще, например, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ. Для ручного же многоалфавитного шифра полагаются лишь на длину и сложность ключа, используя приведенную таблицу, которую можно не держать в тайне, а это упрощает шифрование и расшифровывание.

7. **Использование кодов, таблиц соответствия**. Можно создать таблицу соответствия символов к алфавиту, содержание обеих таблиц может произвольным. Например, такую таблицу, в которой «*» означает какую-нибудь букву, например букву «Д», сочетание и варианты могут быть любыми.

Вопросы и задания к лабораторной работе. Для каждого метода шифрования придумать собственное произвольное зашифрованное сообщение. Знать принципы шифрования описанных методов.

1. Что такое шифрование?

2. Что такое кодирование?

3. В чем разница между кодированием и шифрованием?

4. Виды шифрования?

Жп ронюкжнь м ьлюлц Мтдп

7.4. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Таблица 6

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	менее 41 баллов (неудовлетворительно)	**41-60 баллов (удовлетворительно)**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
ОПК -2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;					
знать: - содержание основных понятий обеспечения информационной безопасности, источники угроз безопасности информации, методы оценки уязвимости информации	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
уметь: - разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: - навыками освоения и внедрения средств защиты	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ОПК-3.Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности					

знать: виды угроз ИС и методы обеспечения информационной безопасности; правовые основы защиты компьютерной информации; стандарты;	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	Билеты к зачету, текущий контроль
уметь: выявлять и оценивать угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС;	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
владеть: навыками работы с различными источниками информации;	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- **для слепых:** задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- **для слабовидящих:** обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;

- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

9.1 Литература

1. Кильдишов В.Д., Использование приложения MS Excel для моделирования различных задач. – М.: СОЛОН-Пресс, 2016. – 156 с.: ил.

2. Операционные системы. Учебник/ под ред. Э.С. Спиридонова, М.С. Клыкова. Изд. Стереотип. – М.: Книжный дом «ЛИБРОКОМ», 2015 – 350 стр.

3. Начальный курс информатики. Часть 2 [Электронный ресурс]: учебное пособие / В. А. Лопушанский, А. С. Борсяков, В. В. Ткач [и др.]. — Электрон. текстовые данные. — Воронеж: Воронежский государственный университет инженерных технологий, 2015. — 75 c. — 978-5-00032-116-4. — Режим доступа: http://www.iprbookshop.ru/47474.html

4. Информационные технологии [Электронный ресурс]: учебник / Ю. Ю. Громов, И. В. Дидрих, О. Г. Иванова [и др.]. — Электрон. текстовые данные. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2015. — 260 c. — 978-5-8265-1428-3. — Режим доступа: http://www.iprbookshop.ru/63852.html

9.2. Методические указания по освоению дисциплины «Информатика». (Приложение)

10. Материально-техническое обеспечение дисциплины

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

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- стационарные компьютеры;
- мультимедийный проектор;
- настенный экран.

10.2. Помещения для самостоятельной работы

Учебная аудитория для самостоятельной работы – 3-07.

Аудитория 3-07, интерактивная доска SB 480-H2-062616, проектор Smart v25, аппаратная Nettop.

Приложение

Методические указания по освоению дисциплины

«*Защита информации*»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Информатика» состоит из двадцати шести связанных между собою разделов, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Информатика» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, лабораторные занятия).
2. Самостоятельная работа студента (подготовка к лекциям, лабораторным занятиям, доклады с презентациями, индивидуальная консультация с преподавателем).

Учебный материал структурирован и изучение дисциплины производится в тематической последовательности. Каждому лабораторному занятию и самостоятельному изучению материала предшествует лекция по данной теме. Обучающиеся самостоятельно проводят предварительную подготовку к занятию, принимают активное и творческое участие в обсуждении теоретических вопросов, разборе проблемных ситуаций и поисков путей их решения.

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10- 15 минут).
2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10-15 минут).
3. В течение недели выбрать время для работы с литературой в электронной библиотечной системе (по 1 часу).

4. При подготовке к лабораторному занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1-2 задачи.

2. Методические указания по работе обучающихся во время проведения лекций

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, прибегать к противопоставлениям и сравнениям, делать обобщения, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к лабораторным занятиям

На лабораторных занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительныйматериал по тематике занятий.

Студенту рекомендуется следующая схема подготовки к лабораторному занятию:

1. Ознакомиться с планом занятия, который отражает содержание предложенной темы.
2. Проработать конспект лекций.
3. Прочитать основную и дополнительную литературу.

В процессе подготовки к лабораторным занятиям, необходимо обратить особоевнимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными

пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение кконкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

1. Ответить на вопросы плана лабораторного занятия.
2. Выполнить домашнее задание.
3. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять практические задания, которые даются в фонде оценочных средств дисциплины.

4. Методические указания обучающимся по организации самостоятельной работы

Цель организации самостоятельной работы по дисциплине «Информатика» – это углубление и расширение знаний в области научной исследовательской деятельности; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к лабораторному занятию включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося,он может подготовить реферат и выступить с ним на практическом занятии. Лабораторное занятие – это, прежде всего, дискуссия, обсуждение конкретной ситуации, то есть предполагает умение внимательно слушать членов малой группы и модератора, а также стараться высказать свое мнение, высказывать собственные идеи и предложения, уточнятьи задавать вопросы коллегам по обсуждению.

При подготовке к контрольной работе (рубежной аттестации) обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий – на лекциях, лабораторных занятиях;
– в контакте с преподавателем вне рамок расписания – на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.
– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ, СРС оценивается в 15 баллов)

1. Доклад с презентацией
2. Подготовка к лабораторным занятиям

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), лабораторных, к изданиям электронных библиотечных систем.

Составитель:

Старший преподаватель кафедры
«Информатика и вычислительная техника» / М.З. Исаева/

СОГЛАСОВАНО:
Зав. выпускающей кафедрой
«Информатика и вычислительная техника» /Э.Д. Алисултанова/

Директор ДУМР / М.А. Магомаева /