МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.В.ДВ	**Криптографические методы защиты информации**

Код направления подготовки	44.03.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Информатика и вычислительная техника
Уровень образования	бакалавр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Старший преподаватель	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	10	13.06.2019	
транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	1	13.09.2020	

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Криптографические методы защиты информации» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.03.04 «Профессиональное обучение (по отраслям)» (уровень образования бакалавр). Дисциплина является дисциплиной по выбору.

1.2 Общая трудоемкость дисциплины составляет 2 з.е., 72 час.

1.3 Изучение дисциплины «Криптографические методы защиты информации» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин: «Аппаратные средства вычислительной техники», «Администрирование информационных систем», «Информатика», «Безопасность жизнедеятельности», «Компьютерные коммуникации и сети», «Основы информационной безопасности», «Правоведение», «Технические средства информатизации».

1.4 Дисциплина «Криптографические методы защиты информации» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Аппаратно-программное обеспечение ИБ», «Информационное право», «Методика обучения информационными технологиями», «Профессиональные компетенции WorldSkills», «Цифровое образование».

1.5 Цель изучения дисциплины:

освоение студентами основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике

1.6 Задачи дисциплины:

1) дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов

2) добиться понимания обучающимися принципов разработки шифров

3) ознакомить с математическими методами, используемыми в криптографии

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

№ п/п	Код и наименование компетенции по ФГОС
	Код и наименование индикатора достижения компетенции
1	ПК-6 способен подбирать методы предпроектного анализа для решения поставленной задачи, методы проектирования необходимого отраслевого обеспечения для решения профессиональных задач
	ПК.6.1 Знать методы предпроектного анализа для решения поставленной задачи.
	ПК.6.2 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.
	ПК.6.3 Владеть методами предпроектного анализа для решения поставленной задачи.

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.6.1 Знать методы предпроектного анализа для решения поставленной задачи.	З.1 • основные задачи и понятия криптографии;требования к шифрам и основные характеристики шифров; модели шифров и математические методы их исследования
2	ПК.6.2 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.	У.1 • применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем
3	ПК.6.3 Владеть методами предпроектного анализа для решения поставленной задачи.	В.1 • навыками использования типовых криптографических алгоритмов

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**				**Итого часов**
	Л	ЛЗ	ПЗ	СРС	
Итого по дисциплине	**12**	**6**	**14**	**40**	**72**
Первый период контроля					
Основные понятия криптографии	***4***	***2***	***6***	***12***	***24***
История криптографии. Исторические шифры	2		2	4	8
Математическая модель шифра. Теория секретности Шеннона.	2		2	4	8
Основные поянтия криптографии		2	2	4	8
Симметричное шифрование	***6***	***4***	***4***	***12***	***26***
Шифры Цезаря, лозунговый шифр, атбаш	2	2		4	8
Шифры перестановки, транспортный, Виженера	2	2		4	8
Шифры гаммирования	2		4	4	10
Асимметричное шифрование и цифровая подпись	***2***		***4***	***16***	***22***
Основные понятяи ассиметричного шифрования: методы, приницп , алгоритмы	2			8	10
Схемы цифровой подписи.			2	4	6
Криптографические протоколы			2	4	6
Итого по видам учебной работы	12	6	14	40	72
Форма промежуточной аттестации					
Зачет					
Итого за Первый период контроля					**72**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные понятия криптографии	***4***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
1.1. История криптографии. Исторические шифры Основные этапы становления криптографии как науки. Классификация шифров. Шифры замены, перестановки, гаммирования. Композиции шифров. Примеры исторических ручных и машинных шифров. Шифр Цезаря. Шифр простой замены. Учебно-методическая литература: 1, 2	2
1.2. Математическая модель шифра. Теория секретности Шеннона. Алгебраическая модель, вероятностная модель. Атаки и угрозы шифрам. Вычислительная и теоретическая стойкость. Теоретико-информационный подход к оценке стойкости шифров. Учебно-методическая литература: 1, 2	2
2. Симметричное шифрование	***6***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	
2.1. Шифры Цезаря, лозунговый шифр, атбаш Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Шифр «Решетка». Шифр Вернама. Enigma. Шифр Хейглина. Учебно-методическая литература: 1, 2	2
2.2. Шифры перестановки, транспортный, Виженера Шифр Виженера. Шифр «Решетка». Шифр Вернама. Enigma. Шифр Хейглина. Способы их вскрытия. Блочные и поточные шифры Учебно-методическая литература: 1, 2	2
2.3. Шифры гаммирования Криптографическая стойкость шифров. Совершенные шифры. Энтропийные характеристики шифров. Идеальные шифры. Избыточность языка. Оценка числа ложных ключей и расстояние единственности. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Учебно-методическая литература: 1, 2	2
3. Асимметричное шифрование и цифровая подпись	***2***
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	
3.1. Основные понятяи ассиметричного шифрования: методы, приницп , алгоритмы Асимметричные (с открытым ключом) шифры. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях. Криптосистема Диффи-Хэллмана. Криптосистемы RSA, Эль-Гамаля, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер. Рюкзачные шифры. Криптосистемы с открытым ключом, основанные на линейных кодах. Преимущества и недостатки асимметричных систем шифрования. Генерация ключевой информации для асимметричных криптосистем. Вероятностные тесты на простоту. Доказуемо простые числа. Нахождение порождающего элемента и элемента заданного порядка. Учебно-методическая литература: 1, 2	2

3.2 Лабораторные

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные понятия криптографии	***2***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	

1.1. Основные поянтия криптографии Криптографические методы защиты информации Цель работы: изучение различных методов защиты информации Теоретическая справка Проблемой защиты информации путем ее преобразования занимается криптология (kryptos – тайный, logos – наука). Криптография занимается поиском и исследованием математических методов преобразования информации. Перечислим основные понятия: Алфавит – конечное множество используемых для кодирования информации знаков. Текст – упорядоченный набор из элементов алфавита. Шифрование – преобразовательный процесс Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный. Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования исходных текстов. Существует много различных методов шифрования. Рассмотрим некоторые из них. Методы перестановки. Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода. Самая простая перестановка – написать исходный текст задом на перед и одновременно разбить шифрограмму на пятерки букв. Например из фразы ПУСТЬ БУДЕТ ТАК КАК МЫ ХОТЕЛИ получим сделаем шифротекст: в исходной фразе до кратности пяти не хватает одной буквы. Допишем в конец любую букву и перевернем фразу: ПУСТЬ БУДЕТ ТАК КАК МЫ ХОТЕЛИО ОИЛЕТ ОХЫМК АККАТ ТЕДУБ БТСУП. Задание. Зашифруйте полученную у преподавателя фразу всеми методами перестановки. Отчет оформите в текстовом редакторе Microsoft Word. Зашифруйте фразу методом гаммирования. Отчет оформите в программе Microsoft Excel. Расшифруйте полученную у преподавателя информацию. Отчет оформите в программе Microsoft Excel. Учебно-методическая литература: 1, 2	2
2. Симметричное шифрование	***4***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	

2.1. Шифры Цезаря, лозунговый шифр, атбаш	2

Шифр Цезаря.
Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве А исходного алфавита сопо-ставляется некоторое множество символов (шифрозамен) МА, Б – МБ, …, Я – МЯ. Шифрозамены выбираются таким образом, чтобы любые два множества (MI и MJ, i □ j) не содержали одинаковых элементов (MI □ MJ = □).
Таблица, приведенная на рис.2, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.

А Б … Я
МА МБ … МЯ

Рис.2. Таблица шифрозамен

При шифровании каждая буква А открытого сообщения заменяется любым символом из множества МА. Если в сообщении содержится не-сколько букв А, то каждая из них заменяется на любой символ из МА. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения.
Так как множества МА, МБ, ..., МЯ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом.
Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»).
Шифры замены можно разделить на следующие подклассы:
- шифры однозначной замены (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 (□Mi□=1 для одного символа);
- полиграммные шифры. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения (□Mi□=1 для блока символов);
- омофонические шифры (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 (□Mi□≥1 для одного символа);
- полиалфавитные шифры (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (□Mi□>1 для одного символа).
Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под алфавитом в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла ( ) и рукопись руни-ческого письма ( ) из романа Ж. Верна «Путешествие к центру Земли».
I. Шифры однозначной замены.
Максимальное количество ключей для любого шифра этого вида не превышает n!, где n – количество символов в алфавите. С увеличением числа n значение n! растет очень быстро (1!=1, 5!=120, 10!=3628800, 15!=1307674368000). При больших n для приближенного вычисления n! можно воспользоваться формулой Стирлинга (3).
Шифр Цезаря. Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (А, Б, ..., Я), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

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

Рис.3. Таблица шифрозамен для шифра Цезаря

При зашифровке буква А заменяется буквой Г, Б - на Д и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними

2.2. Шифры перестановки, транспортный, Виженера Задание на лабораторную работу. В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair; - системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах); - шифра Виженера. При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	2

3.3 Практические

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные понятия криптографии	***6***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	

ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИИ

Разработкой методов преобразования информации с целью обеспе-чения ее конфиденциальности и целостности занимается криптография (в переводе с греческого означает «тайнопись»). О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. С широким распространением письменности криптография стала формироваться как самостоятельная наука.

.рф адукто ,»лон« rfiș .бара то(рфиш - иифарготпирк йитяноп хынвонсо зи ондО ﷺ صِفْر chiffre «цифра» - родственно слову цифра; арабы первыми стали заменять буквы на цифры с целью защиты исходного текста).

Под шифром понимается совокупность методов и способов обратимого преобразования информации с целью ее защиты от НСД.

Шифрование (зашифрование) — процесс применения шифра к за-щищаемой информации, т.е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, шифрограмму, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование — процесс, обратный шифрованию, т. е. преобразо-вание шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Алгоритм криптографического преобразования — набор математических правил, определяющих содержание и последовательность операций, зависящих от ключа шифрования, по шифрованию и дешифрованию информации.

Для шифрования и дешифрования, кроме алгоритма преобразования, необходимо, как правило, знание некоторой секретной информации, которая называется ключом. Ключ шифра (секретный ключ) – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма. В общем случае, ключ – это минимально необходимая информация (за исключением сообщения и алгоритма), необходимая для шифрования и дешифрования сообщений.

Используя понятие ключа, процессы шифрования и дешифрования можно описать в виде соотношений:

$f(P, k1) = C$, (1)

$g(C, k2) = P$, (2)

где P (англ. public - открытый) - открытое сообщение;

C (англ. cipher - шифрованный) - шифрованное сообщение;

f - правило шифрования;

g - правило расшифрования;

k1 – ключ зашифрования, известный отправителю;

k2 – ключ расшифрования, известный адресату.

В зависимости от особенностей алгоритма криптографического преобразования шифры можно разделить на следующие классы.

Криптографические алгоритмы

Одноключевые (симметричные) Двухключевые (асимметричные) Квантовые Комбини-рованные (составные)

Замены (подстановки) Перестановки Аддитивные (гаммирования) Детермини-рованные Вероятностные

Рис.1. Классификация криптографических алгоритмов

В одноключевых системах для шифрования и дешифрования используется один и тот же ключ.

В шифрах перестановки все буквы открытого текста остаются в за-шифрованном сообщении, но меняют свои позиции. В шифрах замены наоборот, позиции букв в шифровке остаются теми же, что и у открытого текста, но символы открытого текста заменяются символами другого ал-фавита.

В аддитивных шифрах буквы алфавита заменяются числами, к кото-рым затем добавляются числа секретной случайной (псевдослучайной) числовой последовательности (гаммы). Состав гаммы меняется в зависимости от используемого ключа. Обычно для шифрования используется логическая операция «Исключающее ИЛИ» (XOR). При дешифровании та же гамма накладывается на зашифрованные

1.2. Математическая модель шифра. Теория секретности Шеннона.	2

Математическая модель шифра замены
Пусть A={μ1, μ2,…,μn} – словосочетания или буквы открытого текста передающей системы, B={λ1,λ2,…,λm} – словосочетания или буквы алфавита шифрования (шифротекста), X – открытый текст сообщения, Y – шифрованное сообщение. Для шифрования текста X выбирается подмножество символов B B, при этом сам текст X является подмножеством символов A A. Таким образом, X A , Y B .

Перед кодированием открытый текст представляется в виде последовательности подслов, называемых шифровеличинами. При шифровании шифровеличины заменяются некоторыми эквивалентами из шифротекста, которые называют шифрообозначениями. И те и другие символы принадлежат элементам

A и B .

Выберем в качестве конкретной реализации передаваемого по сети сооб-

щения (иными словами множество шифровеличин) последовательность симво-

лов A = {μh, μj, …, μk},

а в качестве шифрообозначений B ={λr, λs,…, λl}.

Для определения

правила шифрования Es в общем случае вводится

ряд обозначений и понятие распределителя, который, по сути, будет осуществлять выбор в каждом такте кодирования замену из алфавита B , соответствующей шифровеличине из A .

Представим множество B в виде объединения непустыхподмножеств B*

:

,i

B

w

,

B*

.

B*

,i

1.3. Основные поянтия криптографии Методика и порядок выполнения работы 1. Изучить теоретический материал работы. 2. Провести исследование системы одноалфавитной замены и алгоритма Студенты делятся на две подгруппы. В первой подгруппе студенты выбирают ключевые слова, а так же получают текст, выданный преподавателем. Затем они строят таблицу и осуществляют шифрование текста. Студенты второй подгруппы, получив от студентов первой подгруппы зашифрованное сообщение и необходимый сдвиг, строят таблицу и осуществляют процесс дешифрования. По окончанию расшифрования студенты второй подгруппы приступают к процедуре зашифрования с использованием нового ключевого слова. Студенты первой подгруппы, получив ключевое слово и зашифрованный текст, приступают к его расшифрованию. Содержание отчета и его форма Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы. Вопросы для защиты работы Вопросы к практическому занятию 1. Дайте определение шифра. Какие виды шифров вы знаете. 2. Дайте определение шифра одноалфавитной замены. 3. Назовите основные достоинства и недостатки шифра одноалфавитной замены 4. Дайте определение шифра. Какие виды шифров вы знаете 5. Дайте определение шифра простой подстановки замены 6. Назовите основные достоинства и недостатки шифра Учебно-методическая литература: 1, 2	2
2. Симметричное шифрование	***4***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	

Шифры гаммирования

В аддитивных шифрах используется сложение по модулю (mod) исходного сообщения с гаммой, представленных в числовом виде. Напомним, что результатом сложения двух целых чисел по модулю является остаток от деления (например, 5+10 mod 4 = 15 mod 4 = 3).

В литературе шифры этого класса часто называют потоковыми. Стойкость закрытия этими шифрами определяется, главным образом, качеством гаммы, которое зависит от длины периода и случайности распределения по периоду [1].

Длиною периода гаммы называется минимальное количество символов, после которого последовательность начинает повторяться. Случайность распределения символов по периоду означает отсутствие закономерностей между появлением различных символов в пределах периода.

По длине периода различаются гаммы с конечным и бесконечным периодом. Если длина периода гаммы превышает длину шифруемого текста, гамма является истинно случайной и не используется для шифрования других сообщений, то такое преобразование является абсолютно стойким (совершенный шифр). Такой шифр нельзя вскрыть на основе статистической обработки шифрограммы.

Сложение по модулю N. В 1888 г. француз маркиз де Виари в одной из своих научных статей, посвященных криптографии, доказал, что при замене букв исходного сообщения и ключа на числа справедливы формулы

Ci = (Pi + Ki) mod N, (4)

Pi = (Ci + N - Ki) mod N, (5)

где Pi, Ci - i-ый символ открытого и шифрованного сообщения;

N - количество символов в алфавите;

Ki - i-ый символ гаммы (ключа). Если длина гаммы меньше, чем длина сообщения, то она используется повторно.

Данный метод шифрования воспроизводит зашифрование / расшифрование по Виженеру при замене букв алфавита числами согласно следующей таблице (применительно к русскому алфавиту):

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Щ	Ы	Ь	Ъ	Э	Ю	Я
26	27	28	29	30	31	32

Рис.21. Таблица кодирования символов

Например, для шифрования используется русский алфавит (N = 32, буква Ё эквивалентна Е и не учитывается), открытое сообщение – «АБРАМОВ», гамма – «ЖУРИХИН». При замене символов на числа буква А будет представлена как 0, Б – 1, …, Я – 31. Результат шифрования показан в следующей таблице.

Таблица 2

Пример аддитивного шифрования по модулю N

Символ открытого сообщения, Pi	А	Б	Р	А	М	О	В
	0	1	16	0	12	14	2
гаммы, Ki	Ж	У	Р	И	Х	И	Н
	6	19	16	8	21	8	13
шифрограммы, Ci	Ж	Ф	А	И	Б	Ц	П
	6	20	0	8	1	22	15

Сложение по модулю 2. Является частным случаем предыдущего шифра и используется при шифровании в автоматизированных системах. Символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по модулю 2 (□, для булевых величин аналог этой операции – XOR, «Исключающее ИЛИ»). Процедуры шифрования и дешифрования выполняются по следующим формулам

Ci = Pi □ Ki, (6)

Pi = Ci □ Ki. (7)

Перед иллюстрацией использования шифра приведем таблицу кодов символов Windows 1251 и их двоичное представление.

Таблица 3

Коды символов Windows 1251 и их двоичное представление

Буква	Dec-код	Bin-код	Буква	Dec-код	Bin-код	Буква	Dec-код	Bin-код
А	192	1100 0000	Л	203	1100 1011	Ц	214	1101 0110
Б	193	1100 0001	М	204	1100 1100	Ч	215	1101 0111

3. Асимметричное шифрование и цифровая подпись	*4*
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	
3.1. Схемы цифровой подписи. ИССЛЕДОВАНИЕ ПРОЦЕССА ПОСТРОЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ АЛГОРИТМА RSA С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОЙ РЕАЛИЗАЦИИ Цель и содержание: 1. Углубить знания, по основам использования цифровой подписи асимметричных системах шифрования. 2. Исследовать основные характеристики алгоритма построения электронной подписи на основе RSA Методика и порядок выполнения работы 1. Изучить теоретический материал работы. 2. Провести исследование процедуры построения подписи RSA. Содержание отчета и его форма Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследование процедуры построения цифровой подписи на основе RSA по своему варианту и ответы на вопросы. Вопросы для защиты работы 1. Основные принципы построения цифровых подписей. 2. Основные характеристики построения цифровых подписей на основе алгоритма RSA. 3. Достоинства и недостатки построения цифровой подписи на основе алгоритма RSA. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	2
3.2. Криптографические протоколы Понятие криптографического протокола. Основные примеры. Цель работы: рассмотреть криптографический протокол, как основной обязательный регламент действий участников информационного обмена, позволяющий обеспечить безопасность информационных ресурсов. Задания: для выполнения лабораторной работы необходимо выполнить следующее: 1. Изучить рекомендуемую литературу. 2. Выполнить практическую работу. 3. Ответить на контрольные вопросы. 4. Оформить отчет. Содержание отчета: отчет по лабораторной работе должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине. Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе. В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте. Контрольные вопросы: 1. Понятие криптографического протокола. Основные примеры. 2. Классификация криптографических протоколов. Протоколы сертификации ключей. 3. Протоколы предварительного распределения ключей. 4. Открытое распределение ключей Диффи-Хеллмана и его модификации. Список литературы, рекомендуемый к использованию по данной теме: 1. Шеннон Л.А. Работы по теории информации и кибернетике. М.: ИЛ. 1963. 2. Введение в криптографию. Под ред. В.В. Ященко. Москва, МЦНМО – ЧеРо, 1999. 3. Соловьева Ф.И. Введение в теорию кодирования, учебное пособие для студентов ММФ и ФИТ НГУ. Изд. НГУ, 2006г., 123 с., под грифом УМО. Учебно-методическая литература: 1, 2, 3	2

3.4 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	**Трудоемкость (кол-во часов)**
1. Основные понятия криптографии	***12***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
1.1. История криптографии. Исторические шифры ***Задание для самостоятельного выполнения студентом:*** Подготовка сообщений на тему: 1) Криптография в Древнем мире: Атбаш, Скитала 2) Криптография в Древнем мире: Диск Энея, линейка Энея, книжный шифр 3) Исторические методы стеганографии. 4) Криптография в Средние века: диск Альберти, таблица Тритемия и Виженера. 5) Клод Шеннон и его вклад в криптографию. 6) Алан Тьюринг и его вклад в криптографию. 7) Машина Тьюринга и тест Тьюринга 8) Первый блочный шифр – Lucifer 9) Современная стеганография – математические методы. 10) Электронные водяные знаки. 11) Решетка Кардано. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4
1.2. Математическая модель шифра. Теория секретности Шеннона. ***Задание для самостоятельного выполнения студентом:*** УПРАЖНЕНИЯ. 1. Поясните физический смысл выражения: надежность сообщения должна быть меньше ненадежности ключа. 2. Какая разница между теоретической и практической секретностью с точки зрения отправителя сообщения? С точки зрения криптоаналитика? 3. Какие вопросы для определения теоретической секретности рассматривал К. Шеннон? 4. Какой вопрос рассмотрел К. Шеннон для практической секретности? 5. Приведите классификацию основных методов криптографического закрытия данных. Как вы понимаете их. Учебно-методическая литература: 1, 2, 3	4
1.3. Основные поянтия криптографии ***Задание для самостоятельного выполнения студентом:*** Учебный комплексный проект: «Разработка криптографической программы Задание: разработать программу, реализующую процедуры шифрования и расшифрования по стандарту. Программа должна выдавать промежуточные результаты шифрования/расшифрования. Содержание пояснительной записки. Оглавление 1. Краткие сведения о процедуре шифрования 2.1. Общая схема шифрования. 2.2. Исходный текст процедуры шифрования. 2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы ki, начальная перестановка, полублоки Hi и Li, f(ki, Li), Hi f(ki, Li), конечная перестановка). 3. Руководство пользователя программы. Работа над проектом. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4
2. Симметричное шифрование	***12***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	

2.1. Шифры Цезаря, лозунговый шифр, атбаш ***Задание для самостоятельного выполнения студентом:*** Учебный комплексный проект: «Разработка криптографической программы Задание: разработать программу, реализующую процедуры шифрования и расшифрования по стандарту. Программа должна выдавать промежуточные результаты шифрования/расшифрования. Содержание пояснительной записки. Оглавление 1. Краткие сведения о процедуре шифрования 2.1. Общая схема шифрования. 2.2. Исходный текст процедуры шифрования. 2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы ki, начальная перестановка, полублоки Hi и Li, f(ki, Li), Hi f(ki, Li), конечная перестановка). 3. Руководство пользователя программы. Работа над проектом. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4
2.2. Шифры перестановки, транспортный, Виженера ***Задание для самостоятельного выполнения студентом:*** Учебный комплексный проект: «Разработка криптографической программы Задание: разработать программу, реализующую процедуры шифрования и расшифрования по стандарту. Программа должна выдавать промежуточные результаты шифрования/расшифрования. Содержание пояснительной записки. Оглавление 1. Краткие сведения о процедуре шифрования 2.1. Общая схема шифрования. 2.2. Исходный текст процедуры шифрования. 2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы ki, начальная перестановка, полублоки Hi и Li, f(ki, Li), Hi f(ki, Li), конечная перестановка). 3. Руководство пользователя программы. Работа над проектом. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4
2.3. Шифры гаммирования ***Задание для самостоятельного выполнения студентом:*** Учебный комплексный проект: «Разработка криптографической программы Задание: разработать программу, реализующую процедуры шифрования и расшифрования по стандарту. Программа должна выдавать промежуточные результаты шифрования/расшифрования. Содержание пояснительной записки. Оглавление 1. Краткие сведения о процедуре шифрования 2.1. Общая схема шифрования. 2.2. Исходный текст процедуры шифрования. 2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы ki, начальная перестановка, полублоки Hi и Li, f(ki, Li), Hi f(ki, Li), конечная перестановка). 3. Руководство пользователя программы. Работа над проектом. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4
3. Асимметричное шифрование и цифровая подпись	***16***
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	

3.1.	Основные понятяи ассиметричного шифрования: методы, приницп , алгоритмы ***Задание для самостоятельного выполнения студентом:*** Рассмотреть возможные исходы криптоанализа Изучить методы криптоанализа и их влияние на развитие криптографии Оценить предельные возможности по взлому шифров методом полного перебора ключей Проанализировать применимость различных типов криптоатак к симметричным и асимметричным криптосистемам и хеш-функциям Ознакомиться с перспективными технологиями криптоанализа Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	8
3.2.	Схемы цифровой подписи. ***Задание для самостоятельного выполнения студентом:*** Составить конспект. Схемы формирования ЭЦП, базирующиеся на шифровании с открытым ключом, принципиально уязвимы. Эффективность используемых на практике схем формирования ЭЦП, основанных на криптографии с открытым ключом, с точки зрения быстродействия, является достаточно низкой. Современные практические реализации схем ЭЦП являются уязвимыми. Учитывая бурное развитие вычислительных мощностей современных компьютерных систем и математических методов криптоанализа, практическая схема цифровой подписи должна гарантировать достаточный уровень защиты на годы вперед. При использовании ЭЦП объектом защиты наряду с самим объектом является и его ЭЦП. Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4
3.3.	Криптографические протоколы ***Задание для самостоятельного выполнения студентом:*** Изучить информационные источники [ISO 7498-2:1989] ISO 7498-2:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture: Standard / ISO/IEC JTC 1 Information technology. — 02.1989. — URL: www.iso.org/standard/15841.html. [AVISPA] Automated Validation of Internet Security Protocols and Applications (AVISPA): IST-2001-39252. Deliverable 6.1 ’List of Selected Problems’. Properties (Goals). — 2003. — URL: www.avispa-project.org/delivs/6.1/d6-1/node3.html [Cheremushkin] Черёмушкин А. В. Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика. — 2009. — нояб. — вып. 2. — с. 115—150. — URL: cyberleninka.ru/article/n/kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti.pdf . Учебно-методическая литература: 1, 2, 3 Профессиональные базы данных и информационные справочные системы: 1	4

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
	Основная литература	
1	Бутакова Н.Г. Криптографические методы и средства защиты информации [Электронный ресурс]: учебное пособие/ Бутакова Н.Г., Федоров Н.В.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 384 c.	Режим доступа: http://www.iprbookshop.ru/66791.html.— ЭБС «IPRbooks»
2	Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010.— 95 c.	Режим доступа: http://www.iprbookshop.ru/17925.html.— ЭБС «IPRbooks»
	Дополнительная литература	
3	Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010.— 104 c.	Режим доступа: http://www.iprbookshop.ru/17926.html.— ЭБС «IPRbooks»

4.2. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование базы данных	Ссылка на ресурс
1	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС				
Код образовательного результата дисциплины	Текущий контроль			Промежуточная аттестация
	Опрос	Реферат	Тест	Зачет/Экзамен
ПК-6				
З.1 (ПК.6.1)			+	+
У.1 (ПК.6.2)	+			+
В.1 (ПК.6.3)		+		+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Основные понятия криптографии":

1. Тест

1. Выберите правильный вариант ответа

Криптосистема обладает следующими чертами: предусматривает использование одного и того же закрытого ключа для шифрования и дешифрования данных, характеризуется высокой скоростью работы, но сложностью безопасной передачи самого этого закрытого ключа. Назовите тип криптосистемы.

 Асимметричная криптосистема
 Симметричная криптосистема
 Криптосистема, использующая инфраструктуру открытых ключей (PKI)
 Избыточная криптосистема

2. Выберите правильный вариант ответа

Что из указанного не является предметом изучения криптографии?

 Шифрование с открытым ключом
 Создание алгоритмов надежной электронной подписи
 Метод циклического кода CRC
 Защита передаваемых данных от несанкционированного изменения

3. Выберите все правильные варианты ответов

Укажите все верные утверждения о шифровании данных.

 Любой известный алгоритм шифрования (исключая абсолютно стойкий шифр) можно взломать, перебрав все возможные варианты ключей шифрования
 При сопоставимой криптостойкости длина криптостойкого ключа для симметричного алгоритма шифрования меньше, чем для асимметричного алгоритма
 Современные алгоритмы шифрования ГОСТ 28147-89 (Россия) и AES (США) являются асимметричными
 Асимметричных алгоритмы шифрования работают медленнее по сравнению с симметричными алгоритмами
 Для асимметричных алгоритмов шифрования не известно доказательство нижней оценки их стойкости

4. Выберите правильный вариант ответа

RC4 - это ...

 Алгоритм потокового шифрования (stream cipher)
 Алгоритм блочного шифрования (block cipher)
 Алгоритм асимметричного шифрования (public-key encryption)
 Алгоритм хэширования (hash algorithm)
 Алгоритм создания цифровой подписи (digital signature)

5. Выберите правильный вариант ответа

Для какого алгоритма шифрования типичной является длина ключа 1024 бит?

 RC4
 AES
 3DES
 RSA
 ГОСТ 28147-89

Количество баллов: 5

Типовые задания к разделу "Симметричное шифрование":

1. Опрос

1) Криптография в Древнем мире.
2) Исторические методы стеганографии.
3) Криптография в Средние века и в Новое время.
4) Дисковые шифраторы.
5) Криптография на рубеже 19-20 вв.
6) История отечественной криптографии.

Количество баллов: 5

Типовые задания к разделу "Асимметричное шифрование и цифровая подпись":

1. Реферат

Современная стеганография – математические методы.
Электронные водяные знаки.
Ади Шамир и его вклад в криптографию.
Шифрование и аутентификация в современных беспроводных сетях связи.
Парольные схемы аутентификации.
Одноразовые пароли.
Протоколы с нулевым разглашением.

Количество баллов: 5

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Зачет

Вопросы к зачету:

1. • Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. • Объекты защиты. Категории и носители информации.
3. • Средства защиты информации.
4. • Криптография. Основные термины и определения.
5. • Классификация криптографических систем.
6. • Шифры замены. Классификация и основные методы шифрования.
7. • Шифры перестановки. Классификация и основные методы шифрования.
8. • Шифры гаммирования. Классификация и основные методы шифрования.
9. • Шифры гаммирования. Способы генерации гаммы. Генераторы гамм.
10. • Схема режима шифрования DES-ECB.
11. • Схема режима шифрования DES-CBC.
12. • Схема режима шифрования DES-CPB и DES-OFB.
13. • Тройной DES. Сферы применения различных режимов DES.
14. • Схема режима шифрования простой замены ГОСТ 28147-89.
15. • Шифрование с открытым ключом. Основные понятия.
16. • Алгоритм шифрования RSA.
17. • Алгоритм шифрования Эль-Гамаля.
18. • Алгоритм шифрования на основе задачи об укладке ранца.
19. • Эллиптические кривые. Основные понятия. Сложение и умножение точки.
20. • Алгоритм шифрования на основе эллиптических кривых.
21. • Хэш-функции. Основные понятия и разновидности.
22. • Хэш-функция. MD5.
23. • Криптографические протоколы. Основные понятия.
24. • Протоколы обмена ключами.
25. • Протоколы аутентификации. Разновидности и краткая характеристика.
26. • Парольная идентификация/аутентификация.
27. • Протокол идентификации/аутентификации на основе шифрования с открытым ключом.
28. • Сервер аутентификации Kerberos.
29. • Идентификация/аутентификация с помощью биометрических данных.
30. • Идентификационные карты (ID-cards) и электронные ключи.
31. • Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
32. • ЭЦП на базе алгоритма RSA.
33. • Алгоритм цифровой подписи ГОСТ 34.10-94.
34. • Алгоритм цифровой подписи ГОСТ 34.10-2001.
35. • Протоколы контроля целостности. Разновидности и краткая характеристика.
36. • Протоколы контроля целостности. Биты четности, контрольные цифры и числа.
37. • Протоколы контроля целостности. Использование ЭЦП и MAC-кодов.
38. • Электронные платежи.
39. • Классическое («бумажное») голосования.
40. • Российский опыт электронного голосования.
41. • Протокол разделения секрета.
42. • Протокол подбрасывания монеты по телефону.
43. • Тайные многосторонние вычисления.
44. • Сложность алгоритмов.
45. • Простые числа.
46. • Разложение числа на простые сомножители.
47. • Нахождение начального списка простых чисел.
48. • Тестирование числа на простоту.
49. • Определение наибольшего общего делителя.

50. • Основные сведения о криптоанализе и атаки на криптосистемы.
51. • Классическая стеганография.
52. • Компьютерная стеганография.
53. • Общие сведения о кодировании.
54. • Общедоступные кодовые системы.
55. • Представление чисел в двоичном виде.
56. • Секретные кодовые системы.

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы
"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов
"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2. Лабораторные

Лабораторные занятия проводятся в специально оборудованных лабораториях с применением необходимых средств обучения (лабораторного оборудования, образцов, нормативных и технических документов и т.п.).

При выполнении лабораторных работ проводятся: подготовка оборудования и приборов к работе, изучение методики работы, воспроизведение изучаемого явления, измерение величин, определение соответствующих характеристик и показателей, обработка данных и их анализ, обобщение результатов. В ходе проведения работ используются план работы и таблицы для записей наблюдений.

При выполнении лабораторной работы студент ведет рабочие записи результатов измерений (испытаний), оформляет расчеты, анализирует полученные данные путем установления их соответствия нормам и/или сравнения с известными в литературе данными и/или данными других студентов. Окончательные результаты оформляются в форме заключения.

3. Практические

Практические (семинарские занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения практических занятий и семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

При подготовке к практическому занятию необходимо, ознакомиться с его планом; изучить соответствующие конспекты лекций, главы учебников и методических пособий, разобрать примеры, ознакомиться с дополнительной литературой (справочниками, энциклопедиями, словарями). К наиболее важным и сложным вопросам темы рекомендуется составлять конспекты ответов. Следует готовить все вопросы соответствующего занятия: необходимо уметь давать определения основным понятиям, знать основные положения теории, правила и формулы, предложенные для запоминания к каждой теме.

В ходе практического занятия надо давать конкретные, четкие ответы по существу вопросов, доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

4. Зачет

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

5. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

− проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

− выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

− работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);

− в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

− решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.

− оставить время для проверки ответов, чтобы избежать механических ошибок.

6. Опрос

Опрос представляет собой совокупность развернутых ответов студентов на вопросы, которые они заранее получают от преподавателя. Опрос может проводиться в устной и письменной форме.

Подготовка к опросу включает в себя:

− изучение конспектов лекций, раскрывающих материал, знание которого проверяется опросом;

− повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения;

− изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний;

− составление в мысленной форме ответов на поставленные вопросы.

7. Реферат

Реферат − теоретическое исследование определенной проблемы, включающее обзор соответствующих литературных и других источников.

Реферат обычно включает следующие части:

1. библиографическое описание первичного документа;
2. собственно реферативная часть (текст реферата);
3. справочный аппарат, т.е. дополнительные сведения и примечания (сведения, дополнительно характеризующие первичный документ: число иллюстраций и таблиц, имеющихся в документе, количество источников в списке использованной литературы).

Этапы написания реферата

1. выбрать тему, если она не определена преподавателем;
2. определить источники, с которыми придется работать;
3. изучить, систематизировать и обработать выбранный материал из источников;
4. составить план;
5. написать реферат:

− обосновать актуальность выбранной темы;
− указать исходные данные реферируемого текста (название, где опубликован, в каком году), сведения об авторе (Ф. И. О., специальность, ученая степень, ученое звание);
− сформулировать проблематику выбранной темы;
− привести основные тезисы реферируемого текста и их аргументацию;
− сделать общий вывод по проблеме, заявленной в реферате.

При оформлении реферата следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Проектные технологии
2. Проблемное обучение
3. Развивающее обучение

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. учебная аудитория для семинарских, практических занятий
3. лаборатория
4. Лицензионное программное обеспечение:
   - Операционная система Windows 10
   - Microsoft Office Professional Plus
   - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
   - Справочная правовая система Консультант плюс
   - 7-zip
   - Adobe Acrobat Reader DC