МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (КБГУ)

ИНСТИТУТ ИНФОРМАТИКИ, ЭЛЕКТРОНИКИ И РОБОТОТЕХНИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОГЛАСОВАНО

Руководитель образовательной программы
_____А.С. Ксенофонтов

«___» _____ 2020 г.

УТВЕРЖДАЮ

Директор ИИЭР
_____ Н.В. Черкесова

«___» _____ 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Нальчик 2020

Рабочая программа дисциплины «Теоретические основы криптологии» / сост. С.М. Арванова – Нальчик: ФГБОУ КБГУ, 2020. – 29 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части математического и естественнонаучного цикла студентам очной формы обучения по направлению подготовки 10.03.01. «Информационная безопасность» в 6 семестре.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01. «Информационная безопасность», утвержденного приказом Министерства образования и науки Российской Федерации «01» декабря 2016 г. № 1515.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 4
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО 4
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ 4
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ 6
5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 9
6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ 16
7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 20
7.1. Нормативно-правовая база 20
7.2. Основная литература 20
7.3. Дополнительная литература 20
7.4. Периодические издания 21
7.5. Интернет-ресурсы 21
7.6. Современные профессиональные базы данных 21
7.7. Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы 21
8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 27
ПРИЛОЖЕНИЕ ..... **Ошибка! Закладка не определена.**

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Теоретические основы криптологии» реализует требования федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность».

Целю освоения дисциплины является изучение основных арифметических и алгебраических основ криптографии; изучение криптографических алгоритмов; знакомство с криптографическими методами современных криптосистем.

Задачи: обучение студентов систематизированного представления системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Теоретические основы криптологии» относится к дисциплинам по выбору студентов Б1.Б.19 учебного плана по направлению подготовки ВО 10.03.01 «Информационная безопасность», профиль: Организация и технология защиты информации .

Дисциплине «Теоретические основы криптологии» предшествуют дисциплины: «Математический анализ», «Дискретная математика», «Теория информации и кодирования», «Теоретические основы криптологии».

Освоение данной дисциплины, в свою очередь, необходимо для успешной научной и практической деятельности после окончания университета.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты освоения основной образовательной программы высшего профессионального образования (ОПОП ВО) бакалавриата определяются приобретаемыми выпускником компетенциями, т.е. его способностью применять знания, умения и личные качества в соответствии с задачами профессиональной деятельности.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 10.03.01 «Информационная безопасность»:

а) общепрофессиональными компетенциями (ОПК):

способностью применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2).

б) профессиональными компетенциями (ПК):

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

В результате изучения дисциплины студент должен:

знать:

- как использовать соответствующий математический аппарат при решении профессиональных задач
- соответствующий математический аппарат, применяемый в измерительной технике;
- основы теории множеств, теории соответствий и отношений, теории графов и комбинаторики;

- элементы теории анализа типовых криптографических алгоритмов.
- методы математического и алгоритмического моделирования;
- основные понятия математики, теории дифференциальных уравнений; математические модели простейших систем и процессов в механике и технике.
- методы расчета автоматизированных систем управления;
- соответствующий математический аппарат (элементы теории множеств, элементы теории алгебры логики и логики предикатов и формальных систем основы теории алгоритмов) для решения профессиональных задач;

уметь:

- применять соответствующий математический аппарат при проведении измерительных экспериментов;
- применять математическую символику для выражения количественных и качественных отношений между объектами любой природы;
- использовать методы теории управления для расчета основных параметров информационных систем безопасности в типовых режимах работы,
- применять математические методы при решении профессиональных задач; использовать полученные в процессе изучения курса навыки аналитического и численного решения алгебраических и дифференциальных уравнений и систем, строить математические модели и алгоритмы;
- использовать математические методы при построении криптографических алгоритмов; интерпретировать и применять символический аппарат теории множеств и отношений для описания математических понятий и конструкций,
- применять понятия и алгоритмы теории графов для решения прикладных задач, применять аппарат комбинаторики для решения комбинаторных задач.

владеть:

- навыками использования соответствующего математического аппарата в радиоизмерительной технике; навыками использования соответствующего математического аппарата при решении задач по информационной безопасности;
- навыками составления передаточных функций для заданных схем автоматизированных систем; математическими методами решения профессиональных задач, основными приемами обработки экспериментальных данных, навыками математического и алгоритмического моделирования при решении прикладных задач,
- основными математическими методами и алгоритмами криптографической защиты, символическим аппаратом теории множеств и отношений, основными понятиями теории графов, основными алгоритмами решения задач на графах, понятиями комбинаторики и теории перестановок,
- навыками использования соответствующего математического аппарата при решении профессиональных задач.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

В таблице 1 приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: защита лабораторной работы (ЛР), коллоквиум (К), рубежный контроль (РК), тестирование (Т).

Таблица 1

	Наименование раздела	**Содержание раздела/ темы**	**Код контролируемой компетенции (или ее части)**	**Форма текущего контроля**
1	Введение в криптографию.	Задачи и назначение курса. Краткая история развития криптографии. Основные понятия криптологии. Докомпьютерная криптография.	ПК-1	**К, Т, ЛР**
2	Арифметические основы криптографии.	Алгоритм деления с остатком. Наибольший общий делитель. Взаимно простые числа. Наименьшее общее кратное. Простые числа. Сравнения. Классы вычетов. Функция Эйлера. Сравнения первой степени. Система сравнений первой степени. Первообразные корни. Существование первообразных корней. Индексы по модулям $p^к$ и $2p^к$. Символ Лежандра. Квадратичный закон взаимности. Цепные дроби. Подходящие дроби. Подходящие дроби в качестве наилучших приближений.	ОПК-2	**К, Т, ЛР**
3	Алгебраические основы криптографии.	Понятие группы. Понятие подгрупп. Циклические группы. Гомоморфизм групп. Группы подстановок. Действие группы на множестве. Кольца и поля. Гомоморфизмы колец. Евклидовы кольца. Простые и максимальные идеалы. Конечные расширения полей. Поле разложения. Конечные поля. Порядки неприводимых многочленов. Линейные рекуррентные последовательности. Последовательности максимального периода.	ОПК-2	**К, Т, ЛР**
4	Дополнительные математические элементы криптографии.	Понятие энтропии и ее свойства. Виды энтропии. Источники непрерывных сообщений и их энтропийные свойства.	ОПК-2	**К, Т, ЛР**

		Энтропийная устойчивость. Количество информации. Шенновские модели криптосистем. Оценки стойкости симметричных криптосистем. Односторонние функции. Группы подстановок. Хэш-функции.		
5	Алгоритмы криптографических систем.	Криптосистема DES и ее свойства. Криптосистема IDEA. Криптосистема ГОСТ 28147-89. Алгоритм Rijndael. Криптосистемы с открытым ключом. Общая схема цифровой подписи.	ПК-1	**К, Т, ЛР**

Структура дисциплины

Таблица 2. Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часа).

Вид работы	**Трудоемкость, часы**	
	6 семестр	Всего
Общая трудоемкость (в зачетных единицах)	3	3
Контактная работа (в часах):	45	45
Лекционные занятия (Л)	15	15
Практические занятия (ПЗ)	30	30
Семинарские занятия (СЗ)		
Лабораторные работы (ЛР)		
Самостоятельная работа (в часах):	63	63
Курсовая работа (КР)/ Курсовой проект (КП)		
Самостоятельное изучение разделов/тем	36	36
Подготовка и прохождение промежуточной аттестации	27	27
Вид промежуточной аттестации	экзамен	экзамен

Таблица 3. Лекционные занятия

№ п/п	**Тема**
1.	Задачи и назначение курса. Краткая история развития криптографии. Основные понятия криптологии. Докомпьютерная криптография.
2.	Алгоритм деления с остатком. Наибольший общий делитель. Взаимно простые числа. Наименьшее общее кратное. Простые числа. Сравнения. Классы вычетов. Функция Эйлера. Сравнения первой степени. Система сравнений первой степени. Первообразные корни. Существование первообразных корней. Индексы по модулям $p^к$ и $2p^к$. Символ Лежандра. Квадратичный закон взаимности. Цепные дроби. Подходящие дроби. Подходящие дроби в качестве наилучших приближений.
3.	Понятие группы. Понятие подгрупп. Циклические группы. Гомоморфизм групп. Группы подстановок. Действие группы на множестве. Кольца и поля. Гомоморфизмы колец. Евклидовы кольца. Простые и максимальные идеалы. Конечные расширения полей. Поле разложения. Конечные поля. Порядки

	неприводимых многочленов. Линейные рекуррентные последовательности. Последовательности максимального периода.
4.	Понятие энтропии и ее свойства. Виды энтропии. Источники непрерывных сообщений и их энтропийные свойства. Энтропийная устойчивость. Количество информации. Шенновские модели криптосистем. Оценки стойкости симметричных криптосистем. Односторонние функции. Группы подстановок. Хэш-функции.
5.	Криптосистема DES и ее свойства. Криптосистема IDEA. Криптосистема ГОСТ 28147-89. Алгоритм Rijndael. Криптосистемы с открытым ключом. Общая схема цифровой подписи.

Таблица 4. Практические занятия

№ п/п	Тема
1.	Задачи и назначение курса. Краткая история развития криптографии. Основные понятия криптологии. Докомпьютерная криптография.
2.	Алгоритм деления с остатком. Наибольший общий делитель. Взаимно простые числа. Наименьшее общее кратное. Простые числа. Сравнения. Классы вычетов. Функция Эйлера. Сравнения первой степени. Система сравнений первой степени. Первообразные корни. Существование первообразных корней. Индексы по модулям $p^к$ и $2p^к$. Символ Лежандра. Квадратичный закон взаимности. Цепные дроби. Подходящие дроби. Подходящие дроби в качестве наилучших приближений.
3.	Понятие группы. Понятие подгрупп. Циклические группы. Гомоморфизм групп. Группы подстановок. Действие группы на множестве. Кольца и поля. Гомоморфизмы колец. Евклидовы кольца. Простые и максимальные идеалы. Конечные расширения полей. Поле разложения. Конечные поля. Порядки неприводимых многочленов. Линейные рекуррентные последовательности. Последовательности максимального периода.
4.	Понятие энтропии и ее свойства. Виды энтропии. Источники непрерывных сообщений и их энтропийные свойства. Энтропийная устойчивость. Количество информации. Шенновские модели криптосистем. Оценки стойкости симметричных криптосистем. Односторонние функции. Группы подстановок. Хэш-функции.
5.	Криптосистема DES и ее свойства. Криптосистема IDEA. Криптосистема ГОСТ 28147-89. Алгоритм Rijndael. Криптосистемы с открытым ключом. Общая схема цифровой подписи.

Таблица 5. Самостоятельное изучение разделов дисциплины

№ п/п	Вопросы, выносимые на самостоятельное изучение
1.	Задачи и назначение курса. Краткая история развития криптографии. Основные понятия криптологии. Докомпьютерная криптография.
2.	Алгоритм деления с остатком. Наибольший общий делитель. Взаимно простые числа. Наименьшее общее кратное. Простые числа. Сравнения. Классы вычетов. Функция Эйлера. Сравнения первой степени. Система сравнений первой степени. Первообразные корни. Существование первообразных корней. Индексы по модулям рк и 2рк. Символ Лежандра. Квадратичный закон взаимности. Цепные дроби. Подходящие дроби. Подходящие дроби в качестве наилучших приближений.
3.	Понятие группы. Понятие подгрупп. Циклические группы. Гомоморфизм групп. Группы подстановок. Действие группы на множестве. Кольца и поля. Гомоморфизмы колец. Евклидовы кольца. Простые и максимальные идеалы.

	Конечные расширения полей. Поле разложения. Конечные поля. Порядки неприводимых многочленов. Линейные рекуррентные последовательности. Последовательности максимального периода.
4.	Понятие энтропии и ее свойства. Виды энтропии. Источники непрерывных сообщений и их энтропийные свойства. Энтропийная устойчивость. Количество информации. Шенновские модели криптосистем. Оценки стойкости симметричных криптосистем. Односторонние функции. Группы подстановок. Хэш-функции.
5.	Криптосистема DES и ее свойства. Криптосистема IDEA. Криптосистема ГОСТ 28147-89. Алгоритм Rijndael. Криптосистемы с открытым ключом. Общая схема цифровой подписи.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО И РУБЕЖНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Формы контроля текущих, рубежных и промежуточных знаний студентов по дисциплине определяются в соответствии с учебным планом образовательной программы и в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ.

От обучающихся требуется посещение занятий, выполнение лабораторных работ, знакомство с рекомендованной литературой.

При аттестации обучающихся оценивается качество работы на занятиях (умение вести дискуссию, способность четко и ёмко формулировать свои мысли), уровень подготовки к самостоятельной деятельности, качество выполнения заданий (презентаций, докладов, выполнение лабораторных работ и др.).

Конечными результатами освоения программы дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование этих дескрипторов происходит в течение всего семестра по этапам в рамках различного вида занятий и самостоятельной работы.

5.1. Оценочные материалы для текущего контроля.

Цель текущего контроля – оценка результатов работы в семестре и обеспечение своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы обучающегося. Объектом текущего контроля являются конкретизированные результаты обучения (учебные достижения) по дисциплине.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, оценка качества подготовки на основании выполненных заданий ведется преподавателем (с обсуждением результатов), баллы

Критерии формирования оценок (оценивания) устного опроса

Устный опрос является одним из основных способов учёта знаний обучающегося по дисциплине. Развёрнутый ответ должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения.

В результате устного опроса знания, обучающегося оцениваются по следующей шкале:

3 балла	2 балла	1 балл	0 баллов

ставится, если обучающийся: 1) полно излагает изученный материал, даёт правильное определенное экономических понятий; 2) обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; 3) излагает материал последовательно и правильно с точки зрения норм литературного языка.	ставится, если обучающийся даёт ответ, удовлетворяющий тем же требованиям, что и для балла «1», но допускает 1-2 ошибки, которые сам же исправляет, и 1-2 недочёта в последовательности и языковом оформлении излагаемого.	ставится, если обучающийся обнаруживает знание и понимание основных положений данной темы, но: 1) излагает материал неполно и допускает неточности в определении понятий; 2) не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; 3) излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.	ставится, если обучающийся обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке.

Баллы «1», «2», «3» могут ставиться не только за единовременный ответ, но и за рассредоточенный во времени, т.е. за сумму ответов, данных на протяжении занятия. начисляются в зависимости от сложности задания.

5.2. Оценочные материалы для самостоятельной работы обучающегося (типовые задачи) (при наличии)

Рабочая программа предусматривает проведение лекционных, лабораторных занятий, а также самостоятельную работу обучающихся. В ФГБОУ ВО «Кабардино-Балкарский государственный университет» действует балльно-рейтинговая система оценки учебных достижений, обучающихся по образовательным программам, реализуемым на основании федеральных государственных образовательных стандартов. Балльно-рейтинговая система оценки знаний является одной из составляющих системы управления качеством образовательной деятельности в университете.

Вопросы, выносимые на коллоквиум

(контролируемая компетенция ОПК-2, ПК-1)

Первый коллоквиум

1. В чем особенность асимметричного шифрования данных, отличающая его от симметричного?
2. Каким образом происходит асимметричное шифрование данных?
3. Каким образом происходит создание цифровой подписи сообщения?
4. В чем заключается проверка цифровой подписи сообщения?
5. О чем может свидетельствовать ошибка при проверке цифровой подписи сообщения?

Второй коллоквиум

1. Что такое хеширование?
2. Назовите примеры алгоритмов хеширования.
3. Почему небезопасно использование md5?
4. Назовите примеры атак на алгоритмы хеширования.
5. Что такое имитовставка?

Третий коллоквиум

1. Назовите основные компоненты PKI.
2. Назначение сертификатов.
3. Назовите основные этапы генерации цифрового сертификата.
4. Для чего нужен корневой сертификат?
5. Поясните процесс выпуска сертификата.
6. Обновление сертификата, выработка решения.
7. Отзыв сертификата, выработка решения.
8. Способы запроса сертификата, их отличия.
9. Что произойдет при истечении срока действия корневого сертификата? промежуточного сертификата?
10. Как получить возможность использовать цифровую подпись?
11. Опишите способы получения сертификата.
12. Какие алгоритмы аутентификации используются службами PKI?
13. Какие алгоритмы шифрования используются службами PKI?
14. Опишите возможные иерархические структуры центров сертификации.

Образцы тестовых заданий
(контролируемая компетенция ОПК-2, ПК-1)

Примеры тестовых заданий на 1 точку:

I:
S: … - наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей
+: Криптография
-: Имитозащита
-: Обеспечение конфиденциальности

I:
S: … - это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения
-: Алгоритм
+: Ключ
-: Сертификат

I:
S: В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

- +:механизм безопасности
- -: сервис безопасности

- +: контекст безопасности

Примеры тестовых заданий на 2 точку:

I:
S: … это совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей: $\{Fk : X \rightarrow S, K \in K\}$.
-: Алгоритм
+: Шифр
-: Сертификат

I:
S: … называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.
+: Криптостойкость
-: Имитозащита
-: Гамирование

I:
S: … это завершенная комплексная модель, способная производить двусторонние криптопреобразования над данными произвольного объема и подтверждать время отправки сообщения, обладающая механизмом преобразования паролей и ключей и системой транспортного кодирования.

+: Криптосистема
-: Имитозащита
-: Криптопакет

Примеры тестовых заданий на 3 точку:

I:
S: К … относятся шифр Цезаря, являющийся примером моноалфавитной подстановки, и шифр Виженера, являющийся примером многоалфавитной подстановки.
+: Блочные шифры
-: Поточные шифры
-: Гомофонические шифры

I:
S: … представляют собой разновидность гаммирования и преобразуют открытый текст в шифрованный последовательно по 1 биту..
-: Блочные шифры
+: Поточные шифры
-: Гомофонические шифры

I:
S: Шифры … , или транспозиции, изменяют только порядок следования символов или других элементов исходного текста
-: Замены
+: Перестановки
-: Составные

5.3. Формы и содержание рубежного контроля

Рубежный и промежуточный контроль освоения студентом дисциплины осуществляется в рамках балльно-рейтинговой системы. Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе оценки успеваемости студентов КБГУ приведено в таблице 7.

Таблица 7

Распределение баллов в соответствии с действующим Положением о балльно-рейтинговой системе

№ рейтинговой точки	Коллоквиум	Лаб.практикум	Посещаемость	Тестирование	Итого
1	7	8	3	5	23
2	7	8	3	5	23
3	7	8	4	5	24

Таблица 8

Критерии оценки

Вид мероприятия	Критерии оценки	Баллы
Коллоквиум (устный опрос по теме)	- ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике	0-21 балл
Лабораторное занятие	- понимание цели и задач работы - выполнение заданий и обработка результатов - отчет и защита лабораторной работы	0-24 балла
Компьютерное тестирование по разделам дисциплины	Результаты тестирования (Количество баллов = 5*φ, φ - доля правильно отвеченных тестов по теме).	0-15 баллов
Посещение занятий	При более 3 пропусках без уважительной причины занятий аннулируются баллы	0-10 баллов
Экзамен	ясность, четкость и доказательность изложения ответов на вопросы; - владение специальными терминами; - системность знаний по тематике дисциплины в целом	0-30 баллов
Итоговая оценка		0-100 баллов

Задания для лабораторных занятий

Лабораторный практикум является важным элементом обучения, т.к. прививает навыки самостоятельной работы на различном лабораторном оборудовании и умение пользоваться различными приборами и инструментами.

Пример типовой лабораторной работы «Криптосистема Диффи-Хеллмана»

Целью данной работы является освоить криптосистемы с общим ключом.

Промежуточная аттестация

Список основных вопросов к устному экзамену

(контролируемая компетенция ОПК-2, ПК-1)

1. Определите S -блок и покажите необходимое условие обратимости S -блока.
2. Определите P -блок и перечислите его три варианта. Какой вариант является обратимым?
3. Понятие имитовставки, алгоритм хэширования.
4. Определите составной шифр и перечислите два класса составных шифров.
5. Перечислите два шифра перестановки.
6. Криптосистема Диффи- Хеллмана.
7. Все ли шифры потока являются моноалфавитными? Поясните.
8. Укажите различие между блочным шифром Фейстеля и не-Фейстеля.
9. Определите шифр с симметричным ключом.
10. Укажите различие между синхронным и несинхронным шифрами потока.
11. Криптосистема Эль Гамаля.
12. Списки отзыва сертификатов.
13. Симметричные криптосистемы.
14. Криптографическая файловая система EncFS, ее преимущества и недостатки, криптографическая файловая система EFS.
15. Понятие сетей доверия. Уровни и виды доверия PGP.
16. Криптоконтейнеры.
17. Сертификаты X.509. Сертификаты в OpenSSL.
18. Корневые удостоверяющие центры, цепочки X.509.
19. Перечислите три многоалфавитных шифра.
20. Инфраструктура открытых ключей и OpenSSL.
21. Поясните отличия между шифром потока и блочным шифром.
22. Определите лавинный эффект.
23. Управление сертификатами в OpenSSL, CRL.
24. Почему генератор ключей раунда нуждается в удалении проверочных бит? Обосновать ответ.
25. Разница между слабым ключом, полуслабым ключом и возможно слабым ключом.
26. Цифровой сертификат.
27. Двукратный DES. Атака двукратного DES.
28. Хэширование в OpenSSL.
29. Трехкратный DES. Трехкратный DES с двумя и тремя ключами.
30. Понятие имитовставки, алгоритм хэширования.
31. Перечислите критерии, определенные NIST для AES.
32. Сертификаты в OpenSSL.
33. Перечислите параметры (размер блока, размер ключа и число раундов) для трех версий AES.
34. Перечислите три моноалфавитных шифра.
35. Поясните отличия между моноалфавитным и многоалфавитным шифрами.
36. Сколько преобразований имеется в каждой версии AES?
37. Симметричные и ассиметричные методы шифрования. OpenSSL
38. Сравните DES и AES. Какой из них ориентирован на работу с битом, а какой — на работу с байтом?
39. Определите матрицу состояний в AES.
40. Использование хэш-функций в цифровой подписи.
41. Цифровая подпись.
42. Хеширование.
43. Укажите различие между шифрованием и стеганографией.
44. Проведите анализ расширения ключа AES.
45. Проведите анализ AES: достоинства и недостатки.
46. Определите восемь механизмов безопасности.

47. Определите "лазейку" в односторонней функции и объясните её использование в криптографии с асимметричным ключом.
48. Перечислите и определите пять служб безопасности.
49. Ранцевая криптосистема: односторонняя функция в этой системе, лазейка, открытые и секретные ключи в этой системе. Опишите безопасность этой системы.
50. Укажите различие между пассивными и активными атаками на секретную информацию.
51. Определите три цели безопасности.
52. Криптографическая система RSA. Определите открытые и секретные ключи в этой системе. Опишите безопасность этой системы.

Критерии формирования оценок по промежуточной аттестации

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины.

Методические рекомендации для подготовки к экзамену

Экзамен в 8-м семестре является формой итогового контроля знаний и умений студентов по данной дисциплине, полученных на лекциях, лабораторных занятиях и в процессе самостоятельной работы. К з\экзамену допускаются студенты, набравшие не менее 36 баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену студенты вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка студента к экзамену включает три этапа:

- самостоятельная работа в течение семестра;
- непосредственная подготовка в дни, предшествующие экзамену по темам курса;
- подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену студентам целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в устной форме.

При проведении экзамена в письменной (устной) форме ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенного до сведения студентов накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 20 минут.

При проведении письменного экзамена на работу отводится 60 минут.

Контроль курсовых работ

Курсовые работы не предусмотрены.

6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ

Общий балл текущего и рубежного контроля складывается из следующих составляющих (приложение 2). Критерием оценки уровня сформированности компетенций в рамках учебной дисциплин в 8 семестре является экзамен. Целью промежуточных аттестаций по дисциплине является оценка качества освоения дисциплины обучающимися. Типовые задания, обеспечивающие формирование компетенции ПК-1, ОПК-2 представлены в таблице 9.

Таблица 9. Результаты освоения учебной дисциплины, подлежащие проверке.

Результаты обучения (компетенции)	**Основные показатели оценки результатов обучения**	**Вид оценочного материала**
способность применять соответствующий математический аппарат для решения профессиональных задач (ОПК-2)	*Знать:* как использовать соответствующий математический аппарат при решении профессиональных задач соответствующий математический аппарат, применяемый в измерительной технике; основы теории множеств, теории соответствий и отношений, теории графов и комбинаторики; элементы теории анализа типовых криптографических алгоритмов. методы математического и алгоритмического моделирования; основные понятия математики, теории дифференциальных уравнений; математические модели простейших систем и процессов в механике и технике.	Коллоквиум, Выполнение и защита лабораторных работ, Тестирование (раздел 5)

	методы расчета автоматизированных систем управления; соответствующий математический аппарат (элементы теории множеств, элементы теории алгебры логики и логики предикатов и формальных систем основы теории алгоритмов) для решения профессиональных задач;	
	Уметь: применять соответствующий математический аппарат при проведении измерительных экспериментов; применять математическую символику для выражения количественных и качественных отношений между объектами любой природы; использовать методы теории управления для расчета основных параметров информационных систем безопасности в типовых режимах работы, применять математические методы при решении профессиональных задач; использовать полученные в процессе изучения курса навыки аналитического и численного решения алгебраических и дифференциальных уравнений и систем, строить математические модели и алгоритмы; использовать математические методы при построении криптографических алгоритмов; интерпретировать и применять символический аппарат теории множеств и отношений для описания математических понятий и конструкций, применять понятия и алгоритмы теории графов для решения прикладных задач, применять аппарат комбинаторики для решения комбинаторных задач.	Коллоквиум, Выполнение и защита лабораторных работ, Тестирование (раздел 5)
	Владеть: навыками использования соответствующего математического аппарата в радиоизмерительной технике; навыками использования соответствующего математического аппарата при решении задач по информационной безопасности; навыками составления передаточных функций для заданных схем автоматизированных систем; математическими методами решения профессиональных задач, основными	Коллоквиум, Выполнение и защита лабораторных работ, Тестирование (раздел 5)

	приемами обработки экспериментальных данных, навыками математического и алгоритмического моделирования при решении прикладных задач, основными математическими методами и алгоритмами криптографической защиты, символическим аппаратом теории множеств и отношений, основными понятиями теории графов, основными алгоритмами решения задач на графах, понятиями комбинаторики и теории перестановок, навыками использования соответствующего математического аппарата при решении профессиональных задач.	
способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	*Знать:* правовые аспекты использование СВК, принципы построения СВК, основные структуры и схемотехнику элементов СВК, физические возможности каналов передачи данных СВК, основы схемотехники и элементную базу аналоговых и цифровых электронных устройств, а также архитектуру, положения и инструкции по оформлению технической документации, как произвести даунгрейд ПО программных и программно-аппаратных средств защиты информации; - основные криптографические методы и алгоритмы, используемые в программных, программно-аппаратных и технических средствах защиты информации, основные принципы построения криптоалгоритмов для настройки и обслуживания программно-аппаратных и технических средств, технические средства защиты информации.	Коллоквиум, Выполнение и защита лабораторных работ, Тестирование (раздел 5)
	Уметь: реализовывать алгоритмы типовых задач обеспечения информационной безопасности; составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, проводить анализ предметной области, сочетать элементы системы, проводить экспертную оценку объектов защиты, настраивать комплекс	Коллоквиум, Выполнение и защита лабораторных работ, Тестирование (раздел 5)

	элементов, быстро разобраться в документации к программным, программно-аппаратным и техническим средствам защиты информации - «на месте» произвести апгрейд основных программных модулей программных, программно-аппаратных и технических средств защиты информации, строить и изучать математические модели конкретных явлений и процессов для решения принципиальных задач по обеспечению информационной безопасности программно-аппаратных (в том числе криптографических) и технических средств, использовать компьютеры и аппаратные средства вычислительной техники в средствах защиты информации, выполнять работы по установке, настройке и обслуживанию средств защиты информации.	
	Владеть: способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности; способностью составлять обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности, навыками работы с инструментальными средствами моделирования предметной области, прикладных процессов; навыками использования функциональных и технологических стандартов СВК; работы с инструментальными средствами проектирования СВК, методами, необходимыми для выбора элементной базы и конструкторских решений с учетом требований надежности, устойчивости к воздействию окружающей среды, электромагнитной совместимости и технологичности, навыками по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации борьбы с угрозами, на основе анализа	Коллоквиум, Выполнение и защита лабораторных работ, Тестирование (раздел 5)

	структуры и содержания информационных процессов, целей и задач деятельности программно-аппаратных и технических средств, методами установки, настройки и обслуживанию средств защиты информации.	

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Нормативно-правовая база

1. Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статью 14 Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"»
2. Федеральный закон от 05 апреля 2013 г. № 44-ФЗ (ред. от 31.12.2014) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;
3. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
4. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
5. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
8. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
9. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
10. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
12. Трудовой кодекс РФ. Глава 14. «Защита персональных данных работника».

7.2.Основная литература

1. Кирпичников А.П. Криптографические методы защиты компьютерной информации [Электронный ресурс]: учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Электрон. текстовые данные. — Казань: Казанский национальный исследовательский технологический университет, 2016. — 100 c. — 978-5-7882-2052-9. — Режим доступа: http://www.iprbookshop.ru/79313.html
2. Соколов В.П. Кодирование в системах защиты информации [Электронный ресурс] : учебное пособие / В.П. Соколов, Н.П. Тарасова. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 94 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61485.html
3. Петров А.А. Компьютерная безопасность. Криптографические методы защиты/ А.А. Петров. Саратов: Профобразование, 2017. — 446 c. http://www.iprbookshop.ru /63800.html

7.3.Дополнительная литература

1. Бутакова Н.Г. Криптографические методы и средства защиты информации: учебное пособие / Н.Г. Бутакова, Н.В. Федоров. СПб.: Интермедия, 2017. — 384 с. http://www.iprbookshop.ru/66791.html
2. Жуков А.Е. Системы блочного шифрования: учебное пособие по курсу «Теоретические основы криптологии» / А.Е. Жуков. М. : Московский государственный технический университет имени Н.Э. Баумана, 2013. — 80 с. http://www.iprbookshop.ru/31633.html
3. Тони Хаулет Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям [Электронный ресурс] : учебное пособие / Хаулет Тони. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 608 c. — 978-5-4487-0065-1. — Режим доступа: http://www.iprbookshop.ru/67392.html

7.4.Периодические издания

Журнал – Информационная безопасность

7.5.Интернет-ресурсы

1. Защита от компьютерных вирусов. Антивирусные программы [Электронный ресурс] – www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html
2. Антивирусная защита информации: способы и средства- https://www.google.ru/webhpsourceid=chrome-instant&ion=1&espv

7.6.Современные профессиональные базы данных

1. База данных Science Index (РИНЦ) http://elibrary.ru
2. Национальная электронная библиотека РГБ https://нэб.рф
3. Крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. www.scopus.com

7.7.Методические указания по проведению различных учебных занятий, к курсовому проектированию и другим видам самостоятельной работы

Методические рекомендации при работе над конспектом во время проведения лекции

В процессе лекционных занятий целесообразно конспектировать учебный материал. Для этого используются общие и утвердившиеся в практике правила, и приемы конспектирования лекций:

Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля, на которых делаются пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Целесообразно записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры.

Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами.

Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий.

Методические рекомендации при подготовке к коллоквиуму

- проработать конспекты лекций по вопросам коллоквиума;
- прочитать основную и дополнительную литературу, рекомендованную по изучаемым вопросам;
- ответить на вопросы коллоквиума;
- при затруднениях, проконсультироваться с преподавателем.

Критерии оценивания

Оценка			
неудовлетворительно 2 балла	**удовлетворительно 4 балла**	**хорошо 6 баллов**	**отлично 8 баллов**
Студент не знает значительной части вопросов, допускает существенные ошибки в ответах на вопросы.	Студент поверхностно знает вопросы коллоквиума, допускает неточности в ответе на вопрос	Студент хорошо знает материал, грамотно и по существу излагает его, допуская некоторые неточности в ответе на вопрос.	Студент в полном объеме знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Методические рекомендации по организации самостоятельной работы

Самостоятельная работа (по В.И. Далю «самостоятельный – человек, имеющий свои твердые убеждения») осуществляется при всех формах обучения: очной и заочной.

Самостоятельная работа обучающихся - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процесса преподавателей. Повышение роли самостоятельной работы обучающихся при проведении различных видов учебных занятий предполагает:

– оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих обучающемуся в удобное для него время осваивать учебный материал;

– широкое внедрение компьютеризированного тестирования;

– совершенствование методики проведения практик и научно-исследовательской работы обучающихся, поскольку именно эти виды учебной работы в первую очередь готовят обучающихся к самостоятельному выполнению профессиональных задач;

– модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Самостоятельная работа приводит студента к получению нового знания, упорядочению и углублению имеющихся знаний, формированию у него профессиональных навыков и умений. Самостоятельная работа выполняет ряд функций:

– развивающую;
– информационно-обучающую;
– ориентирующую и стимулирующую;
– воспитывающую;
– исследовательскую.

В рамках курса выполняются следующие виды самостоятельной работы:

1. Проработка учебного материала (по конспектам, учебной и научной литературе);
2. Выполнение разноуровневых задач и заданий;

3. Работа с тестами и вопросами для самопроверки;
4. Выполнение итоговой контрольной работы.

Студентам рекомендуется с самого начала освоения курса работать с литературой и предлагаемыми заданиями в форме подготовки к очередному аудиторному занятию. При этом актуализируются имеющиеся знания, а также создается база для усвоения нового материала, возникают вопросы, ответы на которые студент получает в аудитории.

Необходимо отметить, что некоторые задания для самостоятельной работы по курсу имеют определенную специфику. При освоении курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой. Значительную помощь в подготовке к очередному занятию может оказать имеющийся в учебно-методическом комплексе краткий конспект лекций. Он же может использоваться и для закрепления полученного в аудитории материала. Самостоятельная работа студентов предусмотрена учебным планом и выполняется в обязательном порядке. Задания предложены по каждой изучаемой теме и могут готовиться индивидуально или в группе. По необходимости студент может обращаться за консультацией к преподавателю. Выполнение заданий контролируется и оценивается преподавателем.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач. Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания.

Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории. Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений. Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические рекомендации по работе с литературой

Всю литературу можно разделить на учебники и учебные пособия, оригинальные научные монографические источники, научные публикации в периодической печати. Из них можно выделить литературу основную (рекомендуемую), дополнительную и литературу для углубленного изучения дисциплины.

Изучение дисциплины следует начинать с учебника, поскольку учебник – это книга, в которой изложены основы научных знаний по определенному предмету в соответствии с целями и задачами обучения, установленными программой.

При работе с литературой необходимо учитывать, что имеются различные виды чтения, и каждый из них используется на определенных этапах освоения материала.

Предварительное чтение направлено на выявление в тексте незнакомых терминов и поиск их значения в справочной литературе. В частности, при чтении указанной литературы необходимо подробнейшим образом анализировать понятия.

Сквозное чтение предполагает прочтение материала от начала до конца. Сквозное чтение литературы из приведенного списка дает возможность студенту сформировать свод основных понятий из изучаемой области и свободно владеть ими.

Выборочное – наоборот, имеет целью поиск и отбор материала. В рамках данного курса выборочное чтение, как способ освоения содержания курса, должно использоваться при подготовке к практическим занятиям по соответствующим разделам.

Аналитическое чтение – это критический разбор текста с последующим его конспектированием. Освоение указанных понятий будет наиболее эффективным в том случае, если при чтении текстов студент будет задавать к этим текстам вопросы. Часть из этих вопросов сформулирована в ФОС в перечне вопросов для собеседования. Перечень этих вопросов ограничен, поэтому важно не только содержание вопросов, но сам принцип освоения литературы с помощью вопросов к текстам.

Целью *изучающего* чтения является глубокое и всестороннее понимание учебной информации. Есть несколько приемов изучающего чтения:

1. Чтение по алгоритму предполагает разбиение информации на блоки: название; автор; источник; основная идея текста; фактический материал; анализ текста путем сопоставления имеющихся точек зрения по рассматриваемым вопросам; новизна.
2. Прием постановки вопросов к тексту имеет следующий алгоритм:
   - медленно прочитать текст, стараясь понять смысл изложенного;
   - выделить ключевые слова в тексте;
   - постараться понять основные идеи, подтекст и общий замысел автора.
3. Прием тезирования заключается в формулировании тезисов в виде положений, утверждений, выводов.

К этому можно добавить и иные приемы: прием реферирования, прием комментирования.

Важной составляющей любого солидного научного издания является список литературы, на которую ссылается автор. При возникновении интереса к какой-то обсуждаемой в тексте проблеме всегда есть возможность обратиться к списку относящейся к ней литературы. В этом случае вся проблема как бы разбивается на составляющие части, каждая из которых может изучаться отдельно от других. При этом важно не терять из вида общий контекст и не погружаться чрезмерно в детали, потому что таким образом можно не увидеть главного.

Подготовка к экзамену должна проводиться на основе лекционного материала, материала практических занятий с обязательным обращением к основным учебникам по курсу. Это позволит исключить ошибки в понимании материала, облегчит его осмысление, прокомментирует материал многочисленными примерами.

Методические рекомендации по написанию рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами. Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится

лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда. Процесс написания реферата включает: выбор темы; подбор нормативных актов, специальной литературы и иных источников, их изучение; составление плана; написание текста работы и ее оформление; устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов. Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения. Общий объем реферата 20 листов.

Технические требования к оформлению реферата следующие. Реферат оформляется на листах формата А4, с обязательной нумерацией страниц, причем номер страницы на первом, титульном, листе не ставится. Поля: верхнее, нижнее, правое, левое – 20 мм. Абзацный отступ – 1,25; Рисунки должны создаваться в циклических редакторах или как рисунок Microsoft Word (сгруппированный). Таблицы выполнять табличными ячейками Microsoft Word. Сканирование рисунков и таблиц не допускается. Выравнивание текста (по ширине страницы) необходимо выполнять только стандартными способами, а не с помощью пробелов. Размер текста в рисунках и таблицах – 12 кегль. На титульном листе реферата нужно указать: название учебного заведения, факультета, номер группы и фамилию, имя и отчество автора, тему, место и год его написания. Рекомендуемый объем работы складывается из следующих составляющих: титульный лист (1 страница), содержание (1 страница), введение (1 – 2 страницы), основная часть, которую можно разделить на главы или разделы (10 – 15 страниц), заключение (1 – 3 страницы), список литературы (1 страница), приложение (не обязательно). Если реферат содержит таблицу, то ее номер и название располагаются сверху таблицы, если рисунок, то внизу рисунка.

Содержательные части реферата – это введение, основная часть и заключение. Введение должно содержать рассуждение по поводу того, что рассматриваемая тема актуальна (то есть современна и к ней есть большой интерес в настоящее время), а также постановку цели исследования, которая непосредственно связана с названием работы. Также во введении могут быть поставлены задачи (но не обязательно, так как работа невелика по объему), которые детализируют цель. В заключении пишутся конкретные, содержательные выводы.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7 - 10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения обучающемуся выставляется соответствующая оценка.

Методические рекомендации для подготовки к экзамену:

Экзамен в 7 семестре является формой итогового контроля знаний и умений, обучающихся по данной дисциплине, полученных на лекциях, практических занятиях и в процессе самостоятельной работы. Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой К экзамену допускаются студенты, набравшие 36 и более баллов по итогам текущего и промежуточного контроля. На экзамене студент может набрать от 15 до 30 баллов.

В период подготовки к экзамену обучающиеся вновь обращаются к учебно-методическому материалу и закрепляют промежуточные знания.

Подготовка обучающегося к экзамен включает три этапа:

– самостоятельная работа в течение семестра;
– непосредственная подготовка в дни, предшествующие экзамену по темам курса;
– подготовка к ответу на экзаменационные вопросы.

При подготовке к экзамену обучающимся целесообразно использовать материалы лекций, учебно-методические комплексы, нормативные документы, основную и дополнительную литературу.

На экзамен выносится материал в объеме, предусмотренном рабочей программой учебной дисциплины за семестр. Экзамен проводится в письменной / устной форме.

При проведении экзамена в письменной (устной) форме, ведущий преподаватель составляет экзаменационные билеты, которые включают в себя: тестовые задания; теоретические задания; задачи или ситуации. Формулировка теоретических задания совпадает с формулировкой перечня экзаменационных вопросов, доведенных до сведения обучающихся накануне экзаменационной сессии. Содержание вопросов одного билета относится к различным разделам программы с тем, чтобы более полно охватить материал учебной дисциплины.

В аудитории, где проводится устный экзамен, должно одновременно находиться не более шести студентов на одного преподавателя, принимающего экзамен. На подготовку ответа на билет на экзамене отводится 40 минут.

При проведении письменного экзамена на работу отводиться 60 минут.

Результат устного (письменного) экзамена выражается оценками:

Оценка «отлично»– от 91 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы. Все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному. На экзамене студент демонстрирует глубокие знания предусмотренного программой материала, умеет четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка «хорошо» – от 81 до 90 баллов – теоретическое содержание курса освоено, необходимые практические навыки работы сформированы, выполненные учебные задания содержат незначительные ошибки. На экзамене студент демонстрирует твердое знания основного (программного) материала, умеет четко, грамотно, без существенных неточностей отвечать на поставленные вопросы.

Оценка «удовлетворительно» – от 61 до 80 баллов – теоретическое содержание курса освоено не полностью, необходимые практические навыки работы сформированы частично, выполненные учебные задания содержат грубые ошибки. На экзамене студент демонстрирует знание только основного материала, ответы содержат неточности, слабо аргументированы, нарушена последовательность изложения материала

Оценка «неудовлетворительно» – от 36 до 60 баллов – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий. На экзамене студент демонстрирует незнание значительной части программного материала, существенные ошибки в ответах на вопросы, неумение ориентироваться в материале, незнание основных понятий дисциплины

Методические рекомендации по выполнению лабораторных работ

Выполнение каждой лабораторной работы складывается из следующих этапов.

1. Самостоятельная подготовка студентов к работе. Перед началом работы студенты должны четко представлять себе цель работы, изучить теоретические сведения к лабораторной работе

2. Выполнение работы. Этот этап осуществляется в соответствии с методическими указаниями, которые содержатся в описании к каждой работе. Сформулировать выводы по проделанной работе.

3. Составление отчета о проделанной работе. К отчету о выполненной работе предъявляются следующие требования:

Отчет должен содержать исчерпывающие данные, как о цели работы, так и о результатах в следующей последовательности:

- Титульный лист
- цель работы
- задание на лабораторную работу для своего варианта
- ответы на контрольные вопросы
- результаты выполнения работы
- выводы по работе.

4. Защита лабораторной работы с представлением отчета. Защита лабораторной работы проходит в форме свободной беседы по теме лабораторной работы.

Методические рекомендации по подготовке к тестированию

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся эталоны ответов. При самостоятельной подготовке к тестированию студенту необходимо:

а) готовясь к тестированию, проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

б) четко выясните все условия тестирования заранее. Знать, сколько тестов Вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

в) приступая к работе с тестами, внимательно и до конца прочтите вопрос и предлагаемые варианты ответов. Выберите правильные (их может быть несколько). На отдельном листке ответов выпишите цифру вопроса и буквы, соответствующие правильным ответам;

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

д) если Вы встретили чрезвычайно трудный для Вас вопрос, не тратьте много времени на него. Переходите к другим тестам. Вернитесь к трудному вопросу в конце.

е) обязательно оставьте время для проверки ответов, чтобы избежать механических ошибок.

Критерии оценивания

Оценка			
неудовлетворительно 0 баллов	**удовлетворительно 3 балла**	**хорошо 4 балла**	**отлично 5 баллов**
Менее 50 % правильно выполненных заданий.	50-70% правильно выполненных заданий.	71-85% правильно выполненных заданий.	86-100% правильно выполненных заданий.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к материально-техническому обеспечению

Специализированная аудитория, используемая при проведении занятий лекционного типа №43, №48а, №40, №50, оснащена мультимедийным проектором и комплектом аппаратуры, позволяющей демонстрировать текстовые и графические материалы.

Лаборатории оснащены необходимым оборудованием: Комплект учебного оборудования «Криптографические системы», Учебно-методическими комплексами VipNet, Microsoft Office, 7-zip, Adobe Acrobat Reader DC и др.

Студенты имеют доступ через Интернет доступ к единому образовательному порталу, где в открытом доступе имеются ресурсы учебно-методической литературы, являющиеся разработками ведущих ВУЗов России.

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

Для студентов с ограниченными возможностями здоровья созданы специальные условия для получения образования. В целях доступности получения высшего образования по образовательным программам инвалидами и лицами с ограниченными возможностями здоровья университетом обеспечивается:

1. Альтернативная версия официального сайта в сети «Интернет» для слабовидящих;

2. Для инвалидов с нарушениями зрения (слабовидящие, слепые):

– присутствие ассистента, оказывающего обучающемуся необходимую помощь, дублирование вслух справочной информации о расписании учебных занятий; наличие средств для усиления остаточного зрения, брайлевской компьютерной техники, видеоувеличителей, программ невизуального доступа к информации, программ-синтезаторов речи и других технических средств приема-передачи учебной информации в доступных формах для студентов с нарушениями зрения;

– задания для выполнения на экзамене зачитываются ассистентом;

– письменные задания выполняются на бумаге, надиктовываются ассистенту обучающимся;

3.Для инвалидов и лиц с ограниченными возможностями здоровья по слуху (слабослышащие, глухие):

– на зачете/экзамене присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);

– зачет/экзамен проводится в письменной форме;

4. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, созданы материально-технические условия, обеспечивающие возможность беспрепятственного доступа обучающихся в учебные помещения, объекту питания, туалетные и другие помещения университета, а также пребывания в указанных помещениях (наличие расширенных дверных проемов, поручней и других приспособлений).

– письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

– по желанию студента экзамен проводится в устной форме.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Лист переутверждения рабочей программы дисциплины

Рабочая программа:

одобрена на 2020/2021 учебный год. Протокол № __ заседания кафедры от «__» __ 2020 г.

Разработчик программы_____
Зав. кафедрой_____