Приложение 1 к РПД Защита информации
09.03.02 Информационные системы и технологии
Направленность (профиль) – Программно-аппаратные комплексы
Форма обучения – заочная
Год набора - 2019

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.	Кафедра	Информатики и вычислительной техники
2.	Направление подготовки	09.03.02 Информационные системы и технологии
3.	Направленность (профиль)	Программно-аппаратные комплексы
4.	Дисциплина (модуль)	Защита информации
5.	Форма обучения	заочная
6.	Год набора	2019

1. Методические рекомендации

Приступая к изучению дисциплины, обучающемуся необходимо внимательно ознакомиться с тематическим планом занятий, списком рекомендованной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий. Самостоятельная работа обучающегося предполагает работу с научной и учебной литературой, умение создавать тексты. Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий.

При изучении дисциплины обучающиеся выполняют следующие задания:

– изучают рекомендованную научно-практическую и учебную литературу;
– выполняют задания, предусмотренные для самостоятельной работы.

Основными видами аудиторной работы обучающихся являются лекционные и лабораторные занятия.

1.1. Методические рекомендации по организации работы обучающихся во время проведения лекционных занятий

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на семинарское занятие и указания на самостоятельную работу.

Знакомство с дисциплиной происходит уже на первой лекции, где от обучающегося требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая обучающемуся понять глубинные процессы развития изучаемого предмета как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность обучающегося. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при

самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

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

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

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

1.2. Методические рекомендации по подготовке к лабораторным занятиям.

В процессе обучения, для закрепления изученного материала, необходимо выполнять задания, которые предлагаются в виде лабораторных работ. Список тем, описания работ и примеры оформления результатов работ представлены в рабочей программе дисциплины.

Любая работа должна быть выполнена обучающимся самостоятельно и в срок, указанный преподавателем. Если имеются причины, по которым работа не может быть выполнена, то этот вопрос должен быть разрешен преподавателем по данной дисциплине. Если у обучаемого имеются идеи по улучшению, дополнению или другой модификации работы, то эти идеи должны быть также рассмотрены и оценены преподавателем.

Результаты любой работы должны быть оформлены надлежащим образом. Результаты должны сопровождаться информацией о названии работы, номере варианта, о том кто и когда выполнил работу.

Качество учебной работы обучающихся преподаватель оценивает с использованием технологической карты дисциплины, размещенной на сайте филиала МАГУ.

1.3. Методические рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения.

В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание ученика на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет.

Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого обучающийся знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информации может быть использована при написании текста реферата или другого задания.

Таким образом, при работе с источниками и литературой важно уметь:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прослушанное и прочитанное;

– фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;

– готовить и презентовать развернутые сообщения типа доклада;

– работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;

– пользоваться реферативными и справочными материалами;

– контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;

– обращаться за помощью, дополнительными разъяснениями к преподавателю, другим обучающимся.

– пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);

– использовать при говорении и письме перифраз, синонимичные средства, слова-описания общих понятий, разъяснения, примеры, толкования, «словотворчество»;

– повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;

– обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);

– использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не хватает для выражения тех или иных коммуникативных намерений).

1.4. Методические рекомендации по подготовке к сдаче экзамена

Подготовка к экзамену предполагает изучение теоретических вопросов, рассматриваемых на лекциях. Результатом изучения должно являться понимание основных положений, зафиксированных в списке вопросов, и умение пояснить эти положения «своими словами», но с использованием терминологии данного учебного курса.

Контроль знаний в большей степени практико-ориентированный, - поэтому допуск к ответу на теоретический вопрос осуществляется через проверку практического задания. В качестве практического задания выступают лабораторные работы, а также практический вопрос, входящий в состав экзаменационного билета.

Результаты подготовки практического вопроса необходимо прокомментировать таким образом, чтобы было понятно, как эти результаты были получены.

Результатом подготовки ответа на теоретический вопрос должен быть опорный план-конспект ответа, в котором приведены основные пункты ответа, примеры, схемы и другие поясняющие ответ элементы.

Качество учебной работы обучающихся преподаватель оценивает с использованием технологической карты дисциплины, размещенной на сайте филиала МАГУ.

1.5. Методические рекомендации для занятий в интерактивной форме

В учебном процессе, помимо чтения лекций и аудиторных занятий, используются интерактивные формы. В сочетании с внеаудиторной работой это способствует формированию и развитию профессиональных навыков обучающихся.

Интерактивное обучение представляет собой способ познания, осуществляемый в формах совместной деятельности обучающихся, т.е. все участники образовательного процесса взаимодействуют друг с другом, совместно решают поставленные проблемы, моделируют ситуации, обмениваются информацией, оценивают действие коллег и свое собственное поведение, погружаются в реальную атмосферу делового сотрудничества по разрешению проблем.

В курсе изучаемой дисциплины «Защита информации» в интерактивной форме часы используются в виде: групповых дискуссий.

Тематика занятий с использованием интерактивных форм

№ п/п	Тема	Интерактивная форма	Часы, отводимые на интерактивные формы	
			Лекции	Лабораторные занятия
1.	Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	Групповая дискуссия	-	1
2.	Криптография: шифрование и обеспечение целостности	Групповая дискуссия	-	1
ИТОГО			**2 часа**	

2. Планы лабораторных работ

Лабораторная работа №1. Прототип «Командного процессора» с элементами защиты

Цель работы: реализовать в «командном процессоре» защиту на уровне пользователя с применением метода паролей или его модификаций; реализовать процедуру управления системой защиты на уровне пользователя

Структура командного процессора (блок «защита на уровне пользователя»)
Субъекты: Суперпользователь/администратор, другие пользователи
Объекты: база учетных записей пользователей

Минимальный набор команд:
изменение своего пароля, добавление нового пользователя, удаление пользователя, изменение учетной записи пользователя (изменение логина, дополнительных полей учетной записи (если они есть)), просмотр информации о текущем пользователе, просмотр разрешенной информации о существующих в системе пользователях, несколько нейтральных команд (дата, время, список доступных команд системы и т.п.).

Минимальная функциональность:
пароль не должен быть виден на экране, в системе всегда присутствует хотя бы один суперпользователь, обыкновенный пользователь ограничен в действиях, создаёт новых пользователей (удаляет существующих) только суперпользователь, суперпользователь может изменять пароли всех пользователей, при изменении/добавлении пароля запрашивается его подтверждение, имена пользователей в системе попарно различны (не повторяются), возможность зайти под другим пользователем, не закрывая приложение, работать в системе может только пользователь, успешно прошедший процедуру аутентификации.

Лабораторная работа №2. Криптографические алгоритмы
Цель работы: освоение практических приемов криптографического преобразования информации/
Особенности реализации:
Шифрование. В большинстве случаев необходимо указывать, что шифровать и ключ шифрования.
Расшифрование. Необходимо указывать, что расшифровать и соответствующий ключ.
Модель:
Алгоритмы работы каждого метода, используемого в вариантах данной лабораторной работы, подробно рассматриваются на лекционных занятиях.

Пример возможного алгоритма «Перестановка по матрице»:

0. Ограничения: S=2 – мин размер матрицы, I=7 – макс размер матрицы, E='*'-символы для дополнения;
1. Исходный текст – P, длина текста N символов;
2. Если □N-1 □ S то переход к п.10;
3. Если □N-1 □ I, то K=I Иначе K=□N-1;
4. Используемый ключ: матрица перестановок R (K x K);
5. Выделить очередной блок исходного текста размером K*K;
6. Если блок полностью пустой, то переход к п.11;
7. Если блок не полный, то дополнить символами E;
8. Осуществить перестановку в блоке, согласно матрице R;
9. Переход к п.5;
10. Ошибка: размер сообщения слишком мал;
11. Конец.

Лабораторная работа №3.Использование сторонних криптографических элементов

Цель работы: освоить практические приемы использования компонентов, не включенных в стандартную поставку Delphi или C++Builder (на примере пакета криптографических компонентов DCPcrypt).
Задача: создать приложение, выполняющее функции шифрования и дешифрования файла методом DES, реализованного в библиотеке DCPcrypt (разделения по вариантам нет).
Минимальный набор команд:
a. Шифрование файла методом DES.
b. Расшифрование файла методом DES.
Содержание отчета.
Отчет должен содержать **детальную** последовательность действий при выполнении лабораторной работы.
Рекомендуется выделить два больших раздела «Установка пакета DCPcrypt» и «Создание приложения».
Также перед началом выполнения лабораторной работы настоятельно рекомендуется прочитать параграф 19.1 (*Ch 19.pdf*), где описаны общие принципы использования пакетов в Delphi.
Информацию по установке пакета можно найти в Readme.txt, находящегося в архиве *dcpcrypt2.zip*.
Если используется Borland Developer Studio, то рекомендуется устанавливать пакет в C++Builder.
При создании самого приложения, рекомендуется прочитать документацию к пакету.

Лабораторная работа №4. Стеганография
Тема: Исследование метода компьютерной стеганографии для защиты информации.
Цель работы: освоить практические приемы стеганографического преобразования информации.
Задача: создать приложение, выполняющее две функции: функцию скрытия исходного текста в контейнере стеганографическим методом и функцию извлечения текста из контейнера.
Теоретические сведения, Основные понятия, термины и определения компьютерной стеганографии:
Методы компьютерной стеганографии
Классификация методов
Метод замены младших бит
Метод замены цветовой палитры
Методы текстовой стеганографии