ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники
Кафедра «Информационная безопасность»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДИСЦИПЛИНЫ

Б1.О.34 «Криптографические протоколы»

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 5 Разработка систем защиты информации компьютерных систем объектов информатизации" (по отрасли или в сфере профессиональной деятельности)

ОПОП по специальности:

Компьютерная безопасность

Квалификация выпускника: специалист по защите информации

Форма обучения - очная
Срок обучения — 5,5 лет

Рязань, 2023

Методические рекомендации студентам по освоению дисциплины

Перед началом изучения дисциплины студенту необходимо ознакомиться с содержанием рабочей программы дисциплины, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимися на образовательном портале РГРТУ и сайте кафедры.

Методические рекомендации студентам по работе над конспектом лекции

Работа студента на лекции должна быть направлена на эффективное восприятие излагаемого материала. Поскольку вопросы, рассматриваемые на лекции, в определенной степени связаны с предыдущими темами курса, необходимым условием подготовки к лекции является систематическая работа по освоению курса.

Во время лекции студент должен внимательно слушать лектора и одновременно вести осмысленную запись излагаемого материала, составляя краткий конспект. Умение сосредоточенно слушать лекции, активно воспринимать излагаемые сведения является непременным условием их глубокого и прочного усвоения, а также развития умственных способностей. Конспект является полезным, когда записано самое существенное, основное. Не нужно стремиться записать дословно всю лекцию, и просить лектора несколько раз повторять одну и ту же фразу. Лекция не является уроком-диктантом. Конспектируется только самое важное: формулировки определений и законов, выводы основных уравнений и формул, и то, что старается выделить лектор, на чем акцентирует внимание студентов. Запись лекций рекомендуется вести по возможности собственными формулировками. Целесообразно разработать собственную систему сокращений слов, значки, символы. Тетрадь для конспекта лекций нужно сделать практичной и удобной, так как она является основным информативным и направляющим источником при подготовке к различным занятиям, зачетам и экзаменам. В тетради следует отделить поля, где можно изложить свои мысли и вопросы, появившиеся в ходе лекции. Полезно одну из страниц оставлять свободной для занесения дополнительной информации по данной теме, полученной из других источников. После прослушивания лекции необходимо проработать полученный материал. При работе с конспектом следует пометить материалы, вызывающие затруднения для понимания, и постараться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопросы и обратиться за помощью к преподавателю.

Приступая к изучению той или иной темы (раздела) материала, следует уяснить предмет и исходные положения темы, а также ее взаимосвязь с другими темами.

Планомерная и целенаправленная обработка лекционного материала обеспечивает его надежное закрепление. При работе над изучаемым материалом в

той или иной степени целесообразно использовать различные виды памяти: зрительную (запоминая зрительные образы, иллюстрации, расположение текста), слуховую (перечитывая записи вслух, пересказывая текст) и двигательную (делая выписки, наброски и рисунки).

При изучении теоретической части курса рекомендуется дополнять собственный конспект лекций, материалами из учебника, полученными на консультациях. При этом следует придерживаться плана для описываемой части курса согласно конспекту лекций или учебнику. Составление такого конспекта учит работе с разнообразными источниками, развивает способности выражать свои мысли словами и переносить их на бумагу (и иные носители), позволяет лучше запоминать и понимать материал и существенно упрощает подготовку к зачету и экзамену. В любом случае полезно составление логических схем изучаемого материала. Данный метод способствует детальному осмыслению и обобщению материала. Необходимо регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам. Таким образом, умение слушать лекцию и правильно её конспектировать, систематически, добросовестно и осознанно работать над конспектом с привлечением дополнительных источников – залог успешного усвоения учебного материала. Для осмысленного восприятия теоретического материала рекомендуется заранее ознакомиться с вопросами, рассматриваемыми на лекции.

Методические рекомендации студентам по работе с литературой

В рабочей программе дисциплины для каждого раздела и темы дисциплины указывается основная и дополнительная литература, позволяющая более глубоко изучить данный вопрос. Обычно список всей рекомендуемой литературы преподаватель озвучивает на первой лекции или дает ссылки на ее местонахождение (на образовательном портале РГРТУ, на сайте кафедры и т. д.).

При работе с рекомендуемой литературой целесообразно придерживаться такой последовательности. Сначала лучше прочитать заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом.

Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать.

План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала.

Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:

- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,

- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,

- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,

- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу.

В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации студентам по подготовке к практическим занятиям

Цель практических занятий - способствовать закреплению теоретических знаний, приобретению и развитию практических умений решать задачи, умений и практических навыков применения знаний на практике.

Практические занятия: стимулируют регулярное изучение рекомендованной литературы, а также внимательное отношение к лекционному курсу, закрепляют знания, полученные в процессе лекционного обучения и самостоятельной работы над литературой, расширяют объем профессионально значимых знаний, умений, навыков, позволяют проверить правильность ранее полученных знаний, прививают навыки самостоятельного мышления, устного выступления, способствуют свободному оперированию терминологией, предоставляют преподавателю возможность систематически контролировать уровень самостоятельной работы студентов.

На практических занятиях по криптографическим протоколам рассматриваются:

а) задания-упражнения; б) задания для закрепления и контроля знаний.

Задания-упражнения и задания для контроля знаний рассчитаны на использование готовых теоретических знаний, полученных из книг и лекций. Они помогают студентам приобрести навыки применения полученных знаний для выполнения типовых практических действий.

Методические рекомендации студентам по подготовке к зачету или экзамену

При подготовке к зачету или экзамену студент должен повторно изучить конспекты лекций и рекомендованную литературу, просмотреть результаты проведенных лабораторных работ и практических заданий, а также подготовить ответы на все вопросы, вынесенные на зачет или экзамен.

Необходимо помнить, что практически все зачеты и экзамены в вузе

сконцентрированы в течение короткого временного периода в конце семестра в соответствии с расписанием. Промежутки между очередными зачетами и экзаменами обычно составляют всего несколько дней. Поэтому подготовку к ним нужно начинать заблаговременно в течение семестра. До наступления сессии уточните у преподавателя порядок проведения промежуточной аттестации по его предмету и формулировки критериев для количественной оценивания уровня подготовки студентов. Очень часто для итоговой положительной оценки по предмету необходимо вовремя и с нужным качеством выполнить и защитить лабораторные работы, посетить практические занятия и выполнить соответствующие заданий, т. к. всё это является обязательной частью учебного процесса по данной дисциплине.

Рекомендуется разработать план подготовки к каждому зачету и экзамену, в котором указать, какие вопросы или билеты нужно выучить, какие задачи решить за указанный в плане временной отрезок.

Также бывает полезно вначале изучить более сложные вопросы, а затем переходить к изучению более простых вопросов. При этом желательно в начале каждого следующего дня подготовки бегло освежить в памяти выученный ранее материал.

В период сдачи зачетов и экзаменов организм студента работает в крайне напряженном режиме и для успешной сдачи сессии нужно не забывать о простых, но обязательных правилах:

- по возможности обеспечить достаточную изоляцию: не отвлекаться на разговоры с друзьями, просмотры телепередач, общение в социальных сетях;
- уделять достаточное время сну;
- отказаться от успокоительных. Здоровое волнение – это нормально. Лучше снимать волнение небольшими прогулками, самовнушением;
- внушать себе, что сессия – это не проблема. Это нормальный рабочий процесс. Не накручивайте себя, не создавайте трагедий в своей голове;
- помогите своему организму – обеспечьте ему полноценное питание, давайте ему периоды отдыха с переменой вида деятельности;
- следуйте плану подготовки.

Методические рекомендации студентам по проведению самостоятельной работы

Самостоятельная работа студента над учебным материалом является неотъемлемой частью учебного процесса в вузе.

В учебном процессе образовательного учреждения выделяются два вида самостоятельной работы:

1) аудиторная – выполняется на учебных занятиях, под непосредственным руководством преподавателя и по его заданию), студентам могут быть предложены следующие виды заданий:

– выполнение самостоятельных работ;

– выполнение лабораторных работ;

– выполнение заданий на практических занятиях;

– работу со справочной, нормативной документацией и научной литературой;

– защиту выполненных работ и заданий;

– тестирование и т. д.

2) внеаудиторная – выполняется по заданию преподавателя, но без его непосредственного участия, включает следующие виды деятельности.

– подготовку к аудиторным занятиям (практическим занятиям, лабораторным работам);

– изучение учебного материала, вынесенного на самостоятельную проработку: работа над определенными темами, разделами, вынесенными на самостоятельное изучение в соответствии с рабочими программами учебной дисциплины;

– выполнение домашних заданий разнообразного характера;

– выполнение индивидуальных заданий, направленных на развитие у студентов самостоятельности и инициативы;

– подготовку к учебной и производственной практикам и выполнение заданий, предусмотренных программами практик;

– подготовку зачету, экзамену;

– написание курсовой работы;

– подготовку к ГИА, в том числе выполнение ВКР;

– другие виды внеаудиторной самостоятельной работы, специальные для конкретной учебной дисциплины или профессионального модуля.

Внеаудиторные самостоятельные работы представляют собой логическое продолжение аудиторных занятий, проводятся по заданию преподавателя, который инструктирует студентов и устанавливает сроки выполнения задания.

При планировании заданий для внеаудиторной самостоятельной работы используются следующие типы самостоятельной работы:

– воспроизводящая (репродуктивная), предполагающая алгоритмическую деятельность по образцу в аналогичной ситуации. Включает следующую основную деятельность: самостоятельное прочтение, просмотр, конспектирование учебной литературы, прослушивание записанных лекций, заучивание, пересказ, запоминание, Internet–ресурсы, повторение учебного материала и др.

– реконструктивная, связанная с использованием накопленных знаний и известного способа действия в частично измененной ситуации, предполагает подготовку сообщений, докладов, выступлений на практических занятиях, подбор литературы по дисциплинарным проблемам, написание рефератов, курсовых работ и др.

– эвристическая (частично-поисковая) и творческая, направленная на развитие способностей студентов к исследовательской деятельности. Включает следующие виды деятельности: написание рефератов, научных статей, участие в научно–исследовательской работе, подготовка дипломной работы (проекта), выполнение специальных заданий и др., участие в студенческой научной конференции.

Одной из важных форм самостоятельной работы студента является работа с литературой ко всем видам занятий: лабораторным, практическим, при

подготовке к зачетам, экзаменам, тестированию, участию в научных конференциях.

Один из методов работы с литературой – повторение: прочитанный текст можно заучить наизусть. Простое повторение воздействует на память механически и поверхностно. Полученные таким путем сведения легко забываются.

Более эффективный метод – метод кодирования: прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке. Чтобы основательно обработать информацию и закодировать ее для хранения, важно провести целый ряд мыслительных операций: прокомментировать новые данные; оценить их значение; поставить вопросы; сопоставить полученные сведения с ранее известными. Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения.

Изучение научной учебной и иной литературы требует ведения рабочих записей. Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

План – структура письменной работы, определяющая последовательность изложения материала. Он является наиболее краткой и потому самой доступной и распространенной формой записей содержания исходного источника информации. По существу, это перечень основных вопросов, рассматриваемых в источнике. План может быть простым и развернутым. Их отличие состоит в степени детализации содержания и, соответственно, в объеме.

Преимущество плана состоит в том, что план позволяет наилучшим образом уяснить логику мысли автора, упрощает понимание главных моментов произведения. Кроме того, он позволяет быстро и глубоко проникнуть в сущность построения произведения и, следовательно, гораздо легче ориентироваться в его содержании и быстрее обычного вспомнить прочитанное. С помощью плана гораздо удобнее отыскивать в источнике нужные места, факты, цитаты и т. д.

Выписки представляют собой небольшие фрагменты текста (неполные и полные предложения, отдельные абзацы, а также дословные и близкие к дословным записи об излагаемых в нем фактах), содержащие в себе квинтэссенцию содержания прочитанного. Выписки представляют собой более сложную форму записи содержания исходного источника информации. По сути, выписки – не что иное, как цитаты, заимствованные из текста. Выписки позволяют в концентрированные форме и с максимальной точностью воспроизвести наиболее важные мысли автора. В отдельных случаях – когда это оправдано с точки зрения продолжения работы над текстом – вполне допустимо заменять цитирование изложением, близким дословному.

Тезисы – сжатое изложение содержания изученного материала в утвердительной (реже опровергающей) форме. Отличие тезисов от обычных выписок состоит в том, что тезисам присуща значительно более высокая степень концентрации материала. В тезисах отмечается преобладание выводов над общими рассуждениями. Записываются они близко к оригинальному тексту, т. е. без использования прямого цитирования.

Аннотация – краткое изложение основного содержания исходного источника информации, дающее о нем обобщенное представление. К написанию аннотаций прибегают в тех случаях, когда подлинная ценность и пригодность исходного источника информации исполнителю письменной работы окончательно неясна, но в то же время о нем необходимо оставить краткую запись с обобщающей характеристикой.

Резюме – краткая оценка изученного содержания исходного источника информации, полученная, прежде всего, на основе содержащихся в нем выводов. Резюме весьма сходно по своей сути с аннотацией. Однако, в отличие от последней, текст резюме концентрирует в себе данные не из основного содержания исходного источника информации, а из его заключительной части, прежде всего выводов. Но, как и в случае с аннотацией, резюме излагается своими словами – выдержки из оригинального текста в нем практически не встречаются.

Конспект представляет собой сложную запись содержания исходного текста, включающая в себя заимствования (цитаты) наиболее примечательных мест в сочетании с планом источника, а также сжатый анализ записанного материала и выводы по нему.

При выполнении конспекта требуется внимательно прочитать текст, уточнить в справочной литературе непонятные слова и вынести справочные данные на поля конспекта. Нужно выделить главное, составить план. Затем следует кратко сформулировать основные положения текста, отметить аргументацию автора. Записи материала следует проводить, четко следуя пунктам плана и выражая мысль своими словами. Цитаты должны быть записаны грамотно, учитывать лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля. Необходимо указывать библиографическое описание конспектируемого источника.