

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

Методические указания к самостоятельным работам

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) Информационные системы и технологии в
бизнесе

Квалификация выпускника – бакалавр

Невинномысск 2021

Методические указания предназначены для студентов направления подготовки 09.03.02 Информационные системы и технологии и других технических специальностей. Они содержат рекомендации по организации самостоятельных работ студента для дисциплины «Персональная кибербезопасность».

Методические указания разработаны в соответствии с требованиями ФГОС ВО в части содержания и уровня подготовки выпускников направления 09.03.02 Информационные системы и технологии

Содержание

Введение.....	4
1 Цели задачи самостоятельной работы	4
2 Осваиваемые компетенции	5
3 Приобретаемые знания, умения и навыки.....	5
4 Тематический план занятий	6
5 Задания для самостоятельного изучения	8
6 Подготовка к лекциям.....	10
7 Подготовка к лабораторным работам	11
8 Самостоятельное изучение темы. Конспект.....	12
9 Методические рекомендации по подготовке и прохождению тестирования	15
10 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля).....	15
10.1 Перечень основной литературы:	15
10.2 Перечень дополнительной литературы:	16

Введение

Самостоятельная работа обучающегося является одним из основных методов приобретения и углубления знаний, умений общественной практики. Главной задачей самостоятельной работы является развитие общих и профессиональных компетенций, умений приобретать научные знания путем личных поисков, формирование активного интереса и вкуса к творческому самостоятельному подходу в учебной и практической работе.

Самостоятельная работа студентов – планируемая учебная работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа студентов – это вид учебно-познавательной деятельности, состоящей в индивидуальном, распределенном во времени выполнении студентами комплекса заданий при консультационно координирующей помощи преподавателя, ориентированной на самоорганизацию обучающихся.

Самостоятельная работа направлена на развитие умения обрабатывать и анализировать информацию из разных источников.

Самостоятельная работа складывается из изучения учебной и специальной литературы, как основной, так и дополнительной, нормативного материала, конспектирования источников, подготовки устных и письменных сообщений, докладов, рефератов, выполнения практических ситуационных заданий.

1 Цели задачи самостоятельной работы

Основная цель самостоятельной работы студентов состоит в овладении знаниями, профессиональными умениями и навыками деятельности по направлению подготовки.

Задачами организации самостоятельной работы студентов являются:

- развитие способности работать самостоятельно;
- формирование самостоятельности мышления и принятия решений.
- стимулирование самообразования
- развитие способности планировать и распределять свое время

2 Осваиваемые компетенции

Код	Формулировка
ПК-2	Способен выполнять работы по со-зданию (модификации) и сопровождению ИС, автоматизирующих задач организационного управления и бизнеспроцессов

3 Приобретаемые знания, умения и навыки

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: методы преобразования информации с целью ее защиты при создании (модификации) и сопровождению ИС; принципы работы базовых преобразования информации с целью ее защиты при создании (модификации) и сопровождению ИС	ПК-2
Уметь: решать стандартные задачи преобразования информации с целью ее защиты при создании	ПК-2

(модификации) и сопровождению ИС; применять базовые средства преобразования информации с целью ее защиты при создании (модификации) и сопровождению ИС	
Владеть: навыками анализа профессионально-практической деятельности при преобразовании информации с целью ее защиты при создании (модификации) и сопровождению ИС; навыками реализации базовых средств преобразования информации с целью ее защиты при создании (модификации) и сопровождению ИС	ПК-2

4 Тематический план занятий

Наименование и содержание лекций

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание
1	История развития криптографии 1. История развития криптографии
2	Основные понятия и определения информационной безопасности 1. Основные понятия и определения информационной безопасности
3	Классификация угроз информационной безопасности

	1. Классификация угроз информационной безопасности
4	Методы защиты информации с применением симметричных алгоритмов шифрования 1. основные понятия и определения симметричного шифрования
5	Методы защиты информации с применением симметричных алгоритмов шифрования 1. Шифры перестановки. Анализ шифра простой перестановки. 2. Шифры замены. Анализ шифра замены. 3. Шифр XOR. Анализ шифра XOR.
6	Методы защиты информации с применением асимметричных алгоритмов шифрования 1. Основные понятия и определения асимметричного шифрования
7	Методы защиты информации с применением асимметричных алгоритмов шифрования 1. Шифры основанные на факторизации чисел примеры их реализации.
8	Методы защиты информации с применением методов основанных на разделении данных 1. основные понятия и определения разделения данных 2. методы разделения данных основанные на геометрических законах и численные примеры их реализации
9	Методы защиты информации с применением методов основанных на разделении данных 1. Основные понятия Системы остаточных классов 2. методы разделения данных основанные на системе остаточных классов примеры их реализации

Наименование лабораторных работ

№ дисциплины	Темы Наименование тем лабораторных работ
Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования	
1	Изучение математических моделей шифра простой замены
2	Изучение математических моделей шифра Виженера и численных методов его реализации
3	Изучение математической модели симметричного алгоритма шифрования на примере XOR и численного метода его реализации
Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования	
4	Изучение математической модели ассиметричного алгоритма шифрования и численного метода его реализации на примере алгоритма RSA
Тема 6. Методы защиты информации с применением методов основанных на разделении данных	
5	Изучение математических моделей схем порогового разделение данных, основанных на геометрических законах и численных методов их реализации
6	Изучение математических моделей схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

5 Задания для самостоятельного изучения

Подготовка к лабораторной работе

Изучить следующие темы:

1. Изучение математических моделей шифра простой замены

2. Изучение математических моделей шифра Виженера и численных методов его реализации
3. Изучение математической модели симметричного алгоритма шифрования на примере XOR и численного метода его реализации
4. Изучение математической модели ассиметричного алгоритма шифрования и численного метода его реализации на примере алгоритма RSA
5. Изучение математических моделей схем порогового разделение данных, основанных на геометрических законах и численных методов их реализации
6. Изучение математических моделей схем порогового разделение данных, основанных на системе остаточных классах и численные методы их реализации

Подготовка к лекции

Повторить конспект лекций по изученным темам

Подготовка к тестированию

Повторить проеденный материал

Самостоятельное изучение литературы

Изучить дополнительную литературы по темам:

1. История развития криптографии
2. Основные понятия и определения информационной безопасности
3. Классификация угроз информационной безопасности
4. Методы защиты информации с применением симметричных алгоритмов шифрования
5. Методы защиты информации с применением ассиметричных алгоритмов шифрования
6. Методы защиты информации с применением методов основанных на разделении данных

6 Подготовка к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы. В основу его нужно положить рабочие программы изучаемых в семестре дисциплин.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Слушание и запись лекций – сложный вид вузовской аудиторной работы. Внимательное слушание и конспектирование лекций предполагает интенсивную умственную деятельность студента. Краткие записи лекций, их конспектирование помогает усвоить учебный материал. Конспект является полезным тогда, когда записано самое существенное, основное и сделано это самим студентом. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях.

Конспект лекций лучше подразделять на пункты, параграфы, соблюдая красную строку. Этому в большой степени будут способствовать пункты плана лекции, предложенные преподавателям. Принципиальные места,

определения, формулы и другое следует сопровождать замечаниями «важно», «особо важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек. Лучше если они будут собственными, чтобы не приходилось присить их у однокурсников и тем самым не отвлекать их во время лекции. Целесообразно разработать собственную «маркографию» (значки, символы), сокращения слов. Не лишним будет и изучение основ стенографии. 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 знаниями.

7 Подготовка к лабораторным работам

Для того чтобы лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по рассмотренному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться студентом на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом

порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

8 Самостоятельное изучение темы. Конспект

Конспект – наиболее совершенная и наиболее сложная форма записи. Слово «конспект» происходит от латинского «conspectus», что означает «обзор, изложение». В правильно составленном конспекте обычно выделено самое основное в изучаемом тексте, сосредоточено внимание на наиболее существенном, в кратких и четких формулировках обобщены важные теоретические положения.

Конспект представляет собой относительно подробное, последовательное изложение содержания прочитанного. На первых порах целесообразно в записях ближе держаться тексту, прибегая зачастую к прямому цитированию автора. В дальнейшем, по мере выработки навыков конспектирования, записи будут носить более свободный и сжатый характер.

Конспект книги обычно ведется в тетради. В самом начале конспекта указывается фамилия автора, полное название произведения, издательство, год и место издания. При цитировании обязательная ссылка на страницу книги. Если цитата взята из собрания сочинений, то необходимо указать соответствующий том. Следует помнить, что четкая ссылка на источник – неременное правило конспектирования. Если конспектируется статья, то указывается, где и когда она была напечатана.

Конспект подразделяется на части в соответствии с заранее продуманным планом. Пункты плана записываются в тексте или на полях конспекта. Писать его рекомендуется четко и разборчиво, так как небрежная запись с течением времени становится малопонятной для ее автора. Существует правило: конспект, составленный для себя, должен быть по возможности написан так, чтобы его легко прочитал и кто-либо другой.

Формы конспекта могут быть разными и зависят от его целевого назначения (изучение материала в целом или под определенным углом зрения, подготовка к докладу, выступлению на занятии и т.д.), а также от характера произведения (монография, статья, документ и т.п.). Если речь идет просто об изложении содержания работы, текст конспекта может быть сплошным, с выделением особо важных положений подчеркиванием или различными значками.

В случае, когда не ограничиваются переложением содержания, а фиксируют в конспекте и свои собственные суждения по данному вопросу или дополняют конспект соответствующими материалами их других источников, следует отводить место для такого рода записей. Рекомендуется разделить страницы тетради пополам по вертикали и в левой части вести конспект произведения, а в правой свои дополнительные записи, совмещая их по содержанию.

Конспектирование в большей мере, чем другие виды записей, помогает вырабатывать навыки правильного изложения в письменной форме важные теоретических и практических вопросов, умение четко их формулировать и ясно излагать своими словами.

Таким образом, составление конспекта требует вдумчивой работы, затраты времени и труда. Зато во время конспектирования приобретаются знания, создается фонд записей.

Конспект может быть текстуальным или тематическим. В текстуальном конспекте сохраняется логика и структура изучаемого произведения, а запись ведется в соответствии с расположением материала в книге. За основу

тематического конспекта берется не план произведения, а содержание какой-либо темы или проблемы.

Текстуальный конспект желательно начинать после того, как вся книга прочитана и продумана, но это, к сожалению, не всегда возможно. В первую очередь необходимо составить план произведения письменно или мысленно, поскольку в соответствии с этим планом строится дальнейшая работа. Конспект включает в себя тезисы, которые составляют его основу. Но, в отличие от тезисов, конспект содержит краткую запись не только выводов, но и доказательств, вплоть до фактического материала. Иначе говоря, конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, мыслями и соображениями составителя записи.

Как правило, конспект включает в себя и выписки, но в него могут войти отдельные места, цитируемые дословно, а также факты, примеры, цифры, таблицы и схемы, взятые из книги. Следует помнить, что работа над конспектом только тогда будет творческой, когда она не ограничена текстом изучаемого произведения. Нужно дополнять конспект данными из другими источниками.

В конспекте необходимо выделять отдельные места текста в зависимости от их значимости. Можно пользоваться различными способами: подчеркиваниями, вопросительными и восклицательными знаками, репликами, краткими оценками, писать на полях своих конспектов слова: «важно», «очень важно», «верно», «характерно».

В конспект могут помещаться диаграммы, схемы, таблицы, которые придадут ему наглядность.

Составлению тематического конспекта предшествует тщательное изучение всей литературы, подобранной для раскрытия данной темы. Бывает, что какая-либо тема рассматривается в нескольких главах или в разных местах книги. А в конспекте весь материал, относящийся к теме, будет сосредоточен в одном месте. В плане конспекта рекомендуется делать пометки, к каким источникам (вплоть до страницы) придется обратиться для

раскрытия вопросов. Тематический конспект составляется обычно для того, чтобы глубже изучить определенный вопрос, подготовиться к докладу, лекции или выступлению на семинарском занятии. Такой конспект по содержанию приближается к реферату, докладу по избранной теме, особенно если включает и собственный вклад в изучение проблемы.

9 Методические рекомендации по подготовке и прохождению тестирования

Тесты – это вопросы или задания, предусматривающие конкретный, краткий, четкий ответ на имеющиеся ответы.

При самостоятельной подготовке к тестированию студенту необходимо:

а) проработать информационный материал по дисциплине, предварительно проконсультироваться с ведущим преподавателем по вопросам выбора учебной литературы;

б) выяснить условия тестирования: количество тестовых заданий, количество времени на выполнение тестов, система оценки результатов;

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

10 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

10.1 Перечень основной литературы:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование,

2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87995.html>. — Режим доступа: для авторизир. Пользователей

2. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/98349.html>. — Режим доступа: для авторизир. Пользователей

10.2 Перечень дополнительной литературы:

1. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/104000.html>. — Режим доступа: для авторизир. Пользователей

2. Масюк, М. А. Основные понятия и правовые основы защиты информации : учебное пособие / М. А. Масюк, А. А. Попов, Е. В. Касьянова. — Красноярск : Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, 2020. — 82 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/116643.html>. — Режим доступа: для авторизир. пользователей