Министерство науки и высшего Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
к самостоятельной работе
по дисциплине «Основы информационной безопасности»
для студентов очной формы обучения
направления подготовки 10.03.01 Информационная безопасность

ПЯТИГОРСК
2020 г.

Содержание

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Целью самостоятельной работы студентов является формирование понимания социальной значимости своей будущей профессии, высокой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовности к активной состязательной деятельности в условиях информационного противоборства.

Задачами самостоятельной работы студентов является формирование базовых понятий в области информационной безопасности и защиты информации, осознание места и роли информационной безопасности в системе национальной безопасности РФ и выработка первоначальных практических навыков по защите документов на персональном компьютере.

К видам самостоятельной работы студентов при изучении данной дисциплины относятся:

- самостоятельное изучение темы;
- подготовка к практическим занятиям;
- написание реферата и подготовка по нему доклада с электронной презентацией;
- подготовка к экзамену.

1.1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ ТЕМ И ПОДГОТОВКА К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Самостоятельное изучение темы заключается в углубленном изучении уже разобранной на лекции темы с включением ряда дополнительных вопросов по рекомендованной литературе и интернет-ресурсам.

Подготовка к практическим занятиям заключается в изучении конспекта лекции и параграфа основного рекомендованного учебника (или нескольких источников).

1.2. НАПИСАНИЕ РЕФЕРАТА

Реферат является важной составной частью самостоятельной учебной работы студента и предназначен для углубленного изучения проблематики дисциплины, развития творческих способностей студента.

Задачами работы студента над рефератом являются:

- углубленное изучение выбранной темы;
- приобретение умения вести поиск фактического материала, его анализа и систематизации, формулирования научных выводов;
- приобретение навыков грамотного и логически доказательного изложения текста, правильности оформления работы и приложений.

Реферат представляет собой исследование по отдельной теме (вопросу) дисциплины и пишется, как правило, на основе опубликованных источников и научной литературы. Отражает одну некрупную проблему; умение вести анализ, сравнивать мнения авторов, делать выводы, иметь свою точку зрения.

Одновременно реферат может содержать анализ имеющихся в распоряжении студента нормативных, лекционных и других материалов,

их творческое обобщение и систематизацию. В реферате могут использоваться материалы, полученные в период учебно-исследовательской практики, экскурсий, посещения научных конференций и семинаров. В виде реферата может оформляться доклад студента на практическом занятии. Объем реферата не менее 20 листов.

Результатом работы студента над темой реферата может быть составление определенной схемы, таблицы, графика или расчета.

Для написания реферата студентом используется время, отводимое на самостоятельную работу в объеме 9 часов. Самостоятельная работа студента включает: работу в библиотеке, работу в архиве или сети Интернет, поиск необходимой информации в информационных центрах и информационных сетях учреждений, организаций и предприятий, получение консультаций у преподавателя.

В течение недели студент должен выбрать или сформулировать интересующую его тему, согласовать ее с преподавателем. Студент имеет право предложить тему, не вошедшую в примерную тематику.

Научным руководителем студента при написании реферата является преподаватель, ведущий практические занятия по дисциплине.

Рефераты оцениваются научным руководителем с учетом правильности и полноты исследования темы, доли творческого вклада студента в раскрытие темы, стиля изложения и качества оформления работы. Научный руководитель имеет право вернуть реферат студенту для доработки. Реферат защищается студентом в процессе экзамена. Студенты, не предоставившие научному руководителю готовый реферат, к сдаче экзамена по дисциплине не допускаются.

Оценка за реферат учитывается в числе других показателей текущего контроля при определении итоговой (экзаменационной) оценки по дисциплине.

После написания реферата студент должен подготовить доклад для выступления на практическом занятии и презентацию в пакете MicrosoftPowerPointдля мультимедиа демонстрации во время выступления.

Примерные темы рефератов:

1. Нормативная правовая база информационной безопасности РФ.
2. Становление концептуальных правовых основ информационной безопасности в РФ.
3. Информационные технологии и право.
4. Национальные интересы Российской Федерации в информационной сфере.
5. Состояние информационной безопасности Российской Федерации.
6. Государственная политика обеспечения информационной безопасности РФ.
7. Информация как объект правового регулирования.
8. Правовые основы информационной безопасности личности.
9. Государственная тайна – элемент информационной безопасности

государства.
10. Опасности, подстерегающие пользователя в сети Интернет.
11. Спам – чума XXI века.
12. Оптимизация работы операционной системы.
13. Восстановление информации.
14. Электронные цифровые подписи – новый метод обеспечения информационной безопасности государства.
15. Компьютерные вирусы и их свойства
16. Антивирусные программы.
17. Проактивные системы защиты и системы контроля целостности.
18. Системы отражения атак.
19. Блокирование несанкционированного доступа к компьютеру.
20. Анонимность пользователя в сети Интернет.
21. Комплексная бесплатная защита компьютера.
22. В поисках правильного пароля.
23. Шифрование информации.
24. Аналитическая работа как основа формирования системы защиты информации.
25. Организация работы с персоналом, обладающим конфиденциальной информацией.
26. Ребенок и компьютер.
27. Принцип сохранения данных путем создания резервных копий. Виды Архиваторов и принципы их работы.
28. Защита личных имущественных и неимущественных прав личности в информационной сфере.
29. Профессиональные тайны как подсистема информационной безопасности личности.
30. СМИ как объект информационной безопасности современного общества.

1.3. ПОДГОТОВКА К ЭКЗАМЕНУ

Для подготовки к экзамену студентом используется время, отводимое на самостоятельную работу в объеме 9 часов. Самостоятельная работа студента по подготовке к экзамену включает:

- повторение изученного теоретического материала по вопросам к экзамену, приведенным ниже (20 билетов по 2 теоретических вопроса);
- повторение тем, изученных на практических занятиях, с использованием Методических рекомендаций к практическим занятиям (рекомендуется обратить внимание на переченьзаданий и вопросов для формирования и контроля владения компетенциями, а также на задания для работы на занятии с указаниями глав, параграфов и страниц в указанной ниже литературе).

При подготовке рекомендуется использовать конспекты лекций и приведенную ниже литературу и интернет-ресурсы.

Вопросы к экзамену:

1. Основные понятия (категории) в сфере информации.

2. Основные законы РФ в области компьютерного права, коммерческой тайны и персональных данных.
3. Модель информационной безопасности.
4. Основные составы преступлений в сфере информации.
5. Основные понятия (категории) в области государственной тайны.
6. Перечень сведений, составляющих государственную тайну, и сведений, которые не подлежат засекречиванию.
7. Допуск к государственной тайне.
8. Основные категории в сфере защиты персональных данных.
9. Принципы обработки персональных данных.
10. Защита интеллектуальной собственности.
11. Классификация угроз в сфере защиты информации.
12. Меры обеспечения информационной безопасности.
13. Организационные мероприятия.
14. Организационно-технические и технические мероприятия.
15. Организационная защита информации.
16. Инженерно-техническая защита информации.
17. Аппаратные средства защиты информации.
18. Программные средства защиты информации.
19. Защита от несанкционированного доступа и копирования.
20. Обеспечение информационной безопасности средствами Windows XP.
21. Защита данных в MicrosoftOffice 2007, 2010. Использование цифровой подписи.
22. Понятие компьютерного вируса. История возникновения и причины появления компьютерных вирусов.
23. Разновидности вирусов. Уязвимость программ и пути проникновения вирусов.
24. Принципы работы антивируса, разновидности антивирусных программ и основные меры защиты от вирусов.
25. Проактивные системы защиты, системы контроля целостности и системы отражения атак.
26. Блокирование несанкционированного доступа к компьютеру и принцип действия брандмауэра.
27. Криптографические средства защиты информации.
28. Шифрование речи.
29. Технологии использования паролей.
30. Пресечение разглашения конфиденциальной информации.
31. Защита информации от утечки по техническим каналам.
32. Защита информации от утечки по визуально-оптическим каналам.
33. Защита информации от утечки по акустическим каналам.
34. Защита информации от утечки по электромагнитным каналам.
35. Основные категории в области коммерческой тайны.
36. Законное и незаконное получение конфиденциальной информации.
37. Способы коммерческого шпионажа и обеспечения защиты от него.
38. Политика информационной безопасности компании.
39. Разработка политики информационной безопасности предприятия.
40. Аудит информационной безопасности, основные направления деятельности и этапы проведения аудита.

2. ПЛАН-ГРАФИК ВЫПОЛНЕНИЯ СРС ПО ДИСЦИПЛИНЕ

№	Наименование контрольной точки	Форма контроля	Срок сдачи (недели)
1	**Модель информационной безопасности и правовое регулирование информационной безопасности в РФ**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Участие в семинаре-обсуждении	1
2	**Правовая защита информации и защита информации, отнесенной к государственной тайне**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Тестирование	2
3	**Защита персональных данных**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Участие в дискуссии	3
4	**Угрозы в сфере защиты информации и способы противодействия им**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям*	Тестирование Участие в дискуссии	5
5	**Виды защиты информации**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Тестирование	6
6	**Программные и криптографические средства защиты информации**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Участие в семинаре-обсуждении	14
7	**Защита от утечки информации**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Участие в семинаре-обсуждении	15
8	**Обеспечение сохранности коммерческой тайны**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Участие в дискуссии	17
9	**Аудит информационной безопасности**. - *самостоятельное изучение темы;* - *подготовка к практическим занятиям;*	Тестирование Участие в семинаре-обсуждении	18
	- *написание реферата с подготовкой доклада-презентации;*	Доклад-презентация	
	- *подготовка к экзамену*	Экзамен	19

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ВЫПОЛНЕНИЮ СРС

3.1Название раздела:Модель информационной безопасности и правовое регулирование информационной безопасности в РФ.

3.1.1. Цель – получение базовых теоретических знаний по теме «Модель информационной безопасности и правовое регулирование информационной безопасности в РФ».

3.1.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям-участие в семинаре-обсуждении;
- для написания реферата - выступление с докладом-презентацией.

3.1.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление о характеристиках правовых способов защиты информации, ознакомиться с основными законами РФ в области компьютерного права, коммерческой тайны и персональных данных, выявить и проанализировать структуру модели информационной безопасности РФ. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [1], глава 3, § 3.1, 3.2, стр. 41-44 и приложение 5.

3.2Название раздела:Правовая защита информации и защита информации, отнесенной к государственной тайне.

3.2.1. Цель – получение базовых теоретических знаний по теме «Правовая защита информации и защита информации, отнесенной к государственной тайне».

3.2.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в семинаре-обсуждении.

3.2.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление об основных категориях в области информационной безопасности и государственной тайны, ознакомиться с перечнем сведений, составляющих государственную тайну, проанализироватьосновные составы преступлений в сфере информации. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [1] глава 1, § 1.1, 1.2, стр. 12-19, глава 2, § 2.1-2.3, стр. 20-40 и приложение 4.

3.3Название раздела:Защита персональных данных.

3.3.1. Цель – получение базовых теоретических знаний по теме «Защита

персональных данных».

3.3.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в дискуссии.

3.3.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь понятие о персональных данных, ознакомиться с законом о персональных данных, выявить и проанализировать отечественный и зарубежный опыт защиты персональных данных. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [2], глава 44, § 1-6, стр. 119.

3.4Название раздела:Угрозы в сфере защиты информации и способы противодействия им.

3.4.1. Цель – получение базовых теоретических знаний по теме «Угрозы в сфере защиты информации и способы противодействия им»**.**

3.4.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в дискуссии;
- для написания реферата- выступление с докладом-презентацией.

3.4.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление о видах и классификации угроз конфиденциальной информации, ознакомиться с мерами обеспечения информационной безопасности и с организационными, организационно-техническими и техническими мероприятиями, направленными на ее защиту, выявить и проанализировать способы неправомерного овладения конфиденциальной информацией. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [1], глава 4, § 4.1-4.7, стр. 139-172,[2], глава 4, § 1-3, стр.10-15 и глава 5, § 1, 2, стр. 16, 17.

3.5Название раздела:Виды защиты информации.

3.5.1. Цель – получение базовых теоретических знаний по теме «Виды защиты информации».

3.5.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - устный опрос.

3.5.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление о существующих видах защиты информации, ознакомиться с задачами организационной защиты информации и организационными мероприятиями, проанализировать состав аппаратных средств защиты информации при инженерно-

технической защите информации. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [2], глава 8, § 1-3, стр. 27-29, глава 9, § 1, 2, стр. 30, 31 и глава 10, § 1-3, стр. 32-34.

3.6Название раздела:Программные и криптографические средства защиты информации.

3.6.1. Цель – получение базовых теоретических знаний по теме «Программные и криптографические средства защиты информации».

3.6.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в семинаре-обсуждении;
- для написания реферата - выступление с докладом-презентацией.

3.6.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление о разновидностях существующих средств программной защиты информации, ознакомиться с криптографическими средствами защиты информации, выявить и проанализировать отличительные особенности защиты от несанкционированного доступа, от копирования и от разрушения. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [1], глава 12, § 12.1-12.7, стр. 249-261 и [2], глава 11, § 1-3, стр.35-38,глава 12, § 1, 2, стр. 39,глава 13, § 1-3, стр. 39-40 и глава 14, § 1-3, стр. 41-43.

3.7Название раздела:Защита от утечки информации.

3.7.1. Цель – получение базовых теоретических знаний по теме «Защита от утечки информации».

3.7.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в семинаре-обсуждении;
- для написания реферата - выступление с докладом-презентацией.

3.7.3. Задания для СРС:

- **самостоятельное изучение темы раздела:** студент должен иметь представление о понятиях разглашения и утечки конфиденциальной информации, ознакомиться с мерами защиты информации от утечки по визуально-оптическим, акустическим и электромагнитным каналам, проанализировать особенности перечисленных типов технических каналов утечки. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [2], главы16-24, стр. 46-63.

3.8Название раздела:Обеспечение сохранности коммерческой тайны.

3.8.1. Цель – получение базовых теоретических знаний по теме «Обеспечение сохранности коммерческой тайны»,закрепление навыков решениядифференциальных и интегральных уравнений и систем дифференциальных уравнений операционным методом.

3.8.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в дискуссии;
- для написания реферата - выступление с докладом-презентацией.

3.8.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление об основных категориях в области коммерческой тайны и политике информационной безопасности компании, ознакомиться со способами коммерческого шпионажа и способами защиты от него, выявить и проанализировать способы законного и незаконного получения информации, составляющей коммерческую тайну. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [1], глава 13, § 13.1-13.5, стр. 262-267 и[2], главы25-27, стр. 64-73 и главы36-38, стр.97-101.

3.9Название раздела:Аудит информационной безопасности.

3.9.1. Цель – получение базовых теоретических знаний по теме «Аудит информационной безопасности».

3.9.2. Форма контроля СРС:

- для самостоятельного изучения темы - тестирование;
- для подготовки к практическим занятиям - участие в семинаре-обсуждении;
- для написания реферата - выступление с докладом-презентацией.

3.9.3. Задания для СРС:

- **самостоятельное изучение темы раздела:**студент должен иметь представление об основных направлениях деятельности в области аудита безопасности информации, ознакомиться с этапами проведения аудита, выявить и проанализировать особенности функционирования систем обнаружения компьютерных атак. Для подготовки к этим вопросам студент должен обратиться к следующей литературе: [1], глава 8, § 8.5-8.6, стр. 220-230,[2], глава 32, § 1, 2, стр. 89-91 и глава 33, § 1-3, стр.92-93.

4. ТРЕБОВАНИЯ К ПРЕДСТАВЛЕНИЮ И ОФОРМЛЕНИЮ РЕЗУЛЬТАТОВ СРС

4.1. Требования к оформлению реферата

Реферат подготавливается в текстовом редакторе MicrosoftWord 2007 или 2010, печатается на листах бумаги формата А4 и подшивается в пластиковый скоросшиватель.

Текст реферата должен быть оформлен следующим образом:

- Содержание: Введение, Заключение и минимум – 3 раздела (форматированные как заголовки);
- Объем – 15 – 20 стр.;
- Поля: левое, нижнее – 2см, правое, верхнее – 1,5 см.; красная строка – 1,25см;
- Шрифт: 14 пт., Times New Roman;
- Межстрочный интервал – 1,5; выравнивание – по ширине;
- Нумерация страниц;
- Автоматически средствами Word созданные: оглавление, список литературы (минимум 3 источника) и предметный указатель.

Образец оформления титульного листа реферата приведен в приложении 1.

4.2. Требования к оформлению презентации

Презентация по реферату подготавливается в пакете MicrosoftPowerPoint2007 или 2010 в виде файла типа: Презентация PowerPoint, и предоставляется на проверку в электронном виде на носителе CD или на переносном устройстве на основе Flash-памяти.

Требования к презентации:

- количество слайдов – 15-20;
- презентация должна быть создана либо на основе существующего шаблона, либо с использованием одного из стандартных стилей, представленных в коллекции;
- шрифты заголовков слайдов должны иметь единый стиль оформления;
- презентация должна содержать хотя бы одну иллюстрацию и хотя бы один объект SmartArt;
- ко всем слайдам следует применить эффекты анимации;
- звуковое оформление по желанию студента;
- установка интервалов времени автоматической смены слайдов – по желанию студента.

5. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ

5.1. Рекомендуемая литература.

5.1.1. Основная литература:

1. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия - Телеком, 2006.
2. Ю.С. Сергеева. Защита информации. Конспект лекций. – М.: А-Приор, 2011.

5.1.2. Дополнительная литература:

3. Яремчук С.А. Защита вашего компьютера от сбоев, спама, вирусов и хакеров на 100% (+CD). – СПб.: Питер, 2007.
4. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учеб.пособие. – М.: Финансы и статистика, 2005.
5. Математические и компьютерные основы криптологии: Учеб.пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003.
6. Нечаев В.И. Элементы криптографии (Основы теории защиты информации): Учеб. пособие для ун-тов и пед. вузов / Под ред. В.А. Садовничего – М.: Высш. шк., 1999.
4. Кокс Джойс, Фрай Кертис, Ламберт Стив, Преппернау Джоан, Мюррей Кэтрин. MicrosoftOfficeSystem 2007. Русская версия. Серия «Шаг за шагом»; пер. с англ. – М.: ЭКОМПаблишерз, 2007.

5.2. Интернет-ресурсы:

1. http://www.intuit.ru/department/ds/discrmath - Интернет университет информационных технологий;
2. http://www.studfiles.ru/dir/cat14/subj266/file4146/view34225.html - StudFiles. Все для учебы;
3. http://lib.mexmat.ru/indsearch.php - Электронная библиотека механико-математического факультета МГУ.

ПРИЛОЖЕНИЕ 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

КАФЕДРА КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ И СТАНДАРТИЗАЦИИ

РЕФЕРАТ

ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

НА ТЕМУ:

«…»

РАЗРАБОТАЛ:
СТУДЕНТ___ФИО_____
ГРУППЫ_____

ПРОВЕРИЛ:
ПРЕПОДАВАТЕЛЬ___ФИО_____

Г. ПЯТИГОРСК
20__