Министерство образования и науки Кыргызской Республики

Кыргызский Государственный университет им. И. Арабаева

Факультет Физико-математического образования и информационных технологии

«Утверждаю»
Декан ФФМО и ИТ
...

7.09. 2018

РАБОЧАЯ ПРОГРАММА

По дисциплине: Информационная безопасность в сфере образования

Для магистрантов: 2-курс

По направлению (специальность): **Информационная технология**

Лекции **10** часов **3** семестр **2** курс

Практические (семинарские) занятия _8__ часов _3_ семестр _2_ курс

Лабораторные занятия __часов __ семестр __ курс

Самостоятельная работа _18____ часов _1_ семестр _1_ курс

Курсовая работа ______ семестр

Контрольная работа ___ ___ семестр

Итоговый контроль **3** семестр **2** курс

Рабочая программа составлена на основании:

Кафедра **Прикладная информатика**

Составитель программы: доцент **Канкароева** Алтын Абдыбековна

Обсуждено:
На кафедре
Прикладной информатика
Протокол № 1
«__» ________ 20__ г.
Зав.кафедрой__________

Одобрено:
Учебно-методическим
советом ФФМО и ИТ
Протокол № __
«__» ________ 20__
Председатель УМС ______

Пояснительная записка

В условиях модернизации системы образования одной из основных задач высшей школы является формирование ключевых компетенций будущих выпускников. Компетентностный подход предполагает формирование интеллектуальной и исследовательской культуры студентов и магистрантов, создание условий для самоопределения и самореализации их потенциальных возможностей в процессе обучения.

Курс «Информационная безопасность в сфере образования» позволяет магистрантам ознакомиться с методами и средствами защиты информации в персональном компьютере и компьютерных сетях, изучить способы хранения и шифрования данных, проблемы несанкционированного межсетевого доступа к информации, современные средства криптографической защиты информации, вооружиться методами познания и сформировать познавательную самостоятельность.

1. Цель дисциплины:

- Понимание магистрантами роли и перспектив развития информационных процессов и информатизации общества;
- Ознакомление магистрантов и студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а также с нормативными документами России по данному вопросу и правилами получения соответствующих лицензий.

2. Задачи:

- Проектирование политики информационной безопасности в профессиональной компьютеризированной среде;
- Приобретение практических навыков работы с современными средствами ориентированными программными средствами защиты информации в сетевых средах и использования сетевых ресурсов.

Изучение дисциплины формирует знания и навыки, необходимые специалистам по защите информации и администраторам локальных сетей.

3. Место дисциплины в структуре ООП:

Содержание курса тесно связано с другими дисциплинами учебного плана магистратуры. Курс предназначен для магистрантов первого года обучения, включает в себя 2 зачетных единицы: 108 часов, из них: 4 лекционных, 14 практических, 90 часов- СРС.

Для выполнения поставленных учебных задач предусмотрены две формы организации занятий: лекционная и практическая.

В процессе изучения конкретных тем учебной дисциплины важным является целостность, открытость и адаптивность материала. Поэтому в программе курса кроме вопросов о научном исследовании, структуре, планировании и требованиях к готовой работе предусмотрено ознакомление с элементами речевой компетентности магистрантов, психологического настроя, взаимодействия с аудиторией.

По окончании курса проводится публичная защита реферативной научно-исследования по избранной тематике, выступление, демонстрация уровня психологической готовности магистрантов к представлению результатов работы.

3. Требования к результатам освоения дисциплины:

Магистрант должен знать:

- роли и перспективы развития информационных процессов и информационных технологий общества;
- тенденцией развития информационной безопасности;
- модели возможных угроз;
- терминологию и основные понятия теории безопасности информации;
- нормативные документы России по данному вопросу и правила получения соответствующих лицензий.

Магистрант должен уметь:

- проектировать политику информационной безопасности в профессиональной компьютеризированной среде;
- работать с современными функционально-ориентированными программными средствами защиты информации и использования сетевых ресурсов.

В соответствии с требованиями ГОС ВПО в результате освоения дисциплины обучающийся должен овладеть комплексом компетенций. Выполнение этого требования проверяется при аттестации образовательной программы, в том числе путём контроля остаточных знаний обучающихся.

Таблица 2. Распределение компетенций, формируемых в ходе изучения дисциплины

Коды компетенций	Название компетенции	Форма текущего контроля качества компетенции
ОК-4	способностью использовать знания о современной естественнонаучной картине мира в образовательной и профессиональной деятельности, применять методы математической обработки информации, теоретического и экспериментального исследования	индивидуальное задание, тестирование
ПК-1	способностью применять современные методики и технологии организации и реализации образовательного процесса на различных образовательных ступенях в различных образовательных учреждениях	индивидуальное задание, тестирование
ПК-3	способностью формировать образовательную среду и использовать свои способности в реализации задач инновационной образовательной политики	индивидуальное задание
ПК-4	способностью осуществлять педагогическое сопровождение процессов социализации и профессионального самоопределения обучающихся, подготовки их к сознательному выбору профессии	индивидуальное задание, тестирование
ПК-13	готовностью использовать индивидуальные и групповые технологии принятия решений в управлении образова-	индивидуальное задание, тестирование

	тельным учреждением, опираясь на отечественный и зарубежный опыт	
ПК-14	готовностью к осуществлению педагогического проектирования образовательной среды, образовательных программ и индивидуальных образовательных маршрутов	индивидуальное задание, тестирование
ПК-18	готовностью разрабатывать стратегии просветительской деятельности	индивидуальное задание, тестирование

1. Цели освоения дисциплины

- Понимание роли и перспектив развития информационных процессов и информатизации общества;
- Ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а также с нормативными документами России по данному вопросу и правилами получения соответствующих лицензий

2.Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность» относится к вариативной части общенаучного цикла.

Для освоения дисциплины студенты используют знания и умения, сформированные в ходе изучения предметной области «Информатика» на предыдущем уровне образования.

Освоение данной дисциплины является основой для последующей научно-исследовательской работы студента.

3. Требования к результатам освоения содержания дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО магистратуры по направлению 050100.68 «Педагогическое образование»:

профессиональные компетенции (ПК):

ПК-1 - способностью применять современные методики и технологии организации и реализации образовательного процесса на различных образовательных ступенях в различных образовательных учреждениях

ПК-3 - способностью формировать образовательную среду и использовать свои способности в реализации задач инновационной образовательной политики

ПК-4 - способностью осуществлять педагогическое сопровождение процессов социализации и профессионального самоопределения обучающихся, подготовки их к сознательному выбору профессии

ПК-9 - готовностью к систематизации, обобщению и распространению методического опыта (отечественного и зарубежного) в профессиональной области

ПК-13 - готовностью использовать индивидуальные и групповые технологии принятия решений в управлении образовательным учреждением, опираясь на отечественный и зарубежный опыт

ПК-14 - готовностью к осуществлению педагогического проектирования образовательной среды, образовательных программ и индивидуальных образовательных

маршрутов

ПК-18 - готовностью разрабатывать стратегии просветительской

В результате освоения дисциплины обучающийся должен:

знать:

- Современные методы защиты информации;
- Основные виды угроз;
- Виды продуктов вирусов;
- Формы защиты информации и сетей ЭВМ;
- Требования к защите информации, критерии оценок угроз.

уметь:

- Формулировать тему, проблему, ставить цель и задачи, обосновывать актуальность проблемы, определять гипотезу, доказывать или опровергать ее
- Изготовлять продукт исследовательской деятельности.
- Составлять содержание работы и план своих действий на каждом этапе.
- Составлять структуру своего исследования.
- Проводить исследование и делать выводы по его результатам.
- Работать с различными источниками информации, использовать основные ф защиты информации.
- Выявлять вирусы.
- Использовать современные средства защиты информации.

владеть:

- Навыками защиты научной информации.
- Навыками выявления и уничтожения вирусов дискуссии.
- Навыками защиты сетей ЭВМ от возможных угроз.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. СОДЕРЖАНИЕ ТЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ

№	Наименование темы учебной дисциплины	Лекции
1	2	
1.	Международные стандарты информационного обмена. Понятие угрозы.	2
2.	Информационная безопасность в условиях функционирования в КР глобальных сетей.	2
3.	Виды противников или «нарушителей». Понятие о видах вируса.	2
4.	Три вида возможных нарушений информационной системы. Защита.	2
5.	Основные положения теории информационной безопасности информационных систем.	2
	Итого:	10

4.2.ЛАБОРАТОРНЫЙ ПРАКТИКУМ ИЛИ ПРАКТИКУМ

№	Тема лабораторного занятия	Каб.
1	2	
1.	Международные стандарты информационного обмена. Понятие угрозы.	2
2.	Информационная безопасность в условиях функционирования в КР глобальных сетей.	2
3.	Виды противников или «нарушителей». Понятие о видах вируса.	2
4.	Три вида возможных нарушений информационной системы. Защита.	2
5.	Основные положения теории информационной безопасности информационных систем.	2
	Итого:	8

5. Образовательные технологии

Темы, входящие в содержание курса, транслируются в форме лекций. В процессе лекций, укрупненные дидактические единицы передаются в информационном режиме для достижения глобальных целей воспитания и развития.

На занятиях *лабораторного* цикла каждый студент получает индивидуальное задание, направленное на формирование компетенций определенных данной рабочей программой. Во время выполнения заданий в учебной аудитории студент может *консультироваться* с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания осталась не выполненной, студент может продолжить её выполнение во время внеаудиторной *самостоятельной* работы.

Для оценивания результатов изучения дисциплины используется балльно-рейтинговая *система*.

Выполнение всех лабораторных и контрольных работ.

Зачет так же можно получить по рейтинговым баллам, набрав 60 баллов.

Баллы рейтинга

20 баллов – посещение всех лекций
10 баллов – выполнение всех лабораторных работ
25 баллов – защита всех лабораторных работ
30 баллов – СРС

В СРС входит:

1. Подготовка конспекта теоретического вопроса по СРС.
2. Участие в НИРС по дисциплине:
3. Написание реферата по заданной теме:
4. Доклады (сообщения) на научно-практических и др. конференциях, подготовка тезисов для публикации;

6. Содержание форм, методов, средств организации образовательного процесса

6.1.Темы лекционных занятий

Лекция № 1. Международные стандарты информационного обмена. Понятие угрозы.

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия. Механизмы безопасности. Классы безопасности. Основные определения и критерии классификации угроз.

Лекция № 2. Информационная безопасность в условиях функционирования в России глобальных сетей.

Понятие информационной безопасности. Основные составляющие информационную безопасность. Важность и сложность проблемы информационной безопасности в условиях функционирования в КР глобальных сетей.

Лекция № 3. Виды противников или «нарушителей». Понятие о видах угроз.

Угроза - потенциальная возможность определенным способом нарушить ИБ. Угрозы информационной безопасности классифицируются

Лекция № 4. Три вида возможных нарушений информационной системы. Канал:

Несанкционированный доступ

Основной этап (разведывательный, диверсионный)

Скрытая передача информации

Лекция № 5. Основные положения теории информационной безопасности информационных систем.

Надежная защита в информационном пространстве информационного обеспечения и предупреждение искажения, уничтожения, несанкционированной модификации злоумышленного получения и использования информации.

6.2.Темы лабораторных занятий.

Практическое занятие № 1. Международные стандарты информационного обмена. Понятие угрозы

Цель работы: Получение знаний о видах угроз, путей и каналов утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками.

Рекомендации к самостоятельной работе:

Повторить лекционный материал по теме «Международные стандарты информационного обмена. Понятие угрозы».

Изучив тему, студент должен:

- знать закономерности возникновения угроз информационной безопасности;
- знать классификацию угроз информационной безопасности;
- знать пути и каналы утечки информации;
- знать виды удаленных атак на интрасеть;
- знать классические и современные методы взлома интрасетей.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

угроза информационной безопасности, утечка информации, нарушение целостности информации, модификация информации, искажение информации, подделка информации, уничтожение информации, блокирование информации, побочное электромагнитное излучение, электромагнитная наводка, специальное электронное закладное устройство, внешнее воздействие на информационный ресурс.

Содержание работы:

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Виды атак и методы взлома интрасетей»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Основные закономерности возникновения и классификация угроз информационной безопасности.
2. Пути и каналы утечки информации.
3. Удаленные атаки на интрасети.
4. Классические методы взлома интрасетей.
5. Современные методы взлома интрасетей.

Методические указания по изучению вопросов темы

При изучении вопроса 1:

- читать учебное пособие «Информационная безопасность»;
- принять участие в форуме по теме «Виды атак и методы взлома интрасетей»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.compulenta.ru, www.isecurity.ru,www.oxpaha.ru, www.cyberterrorism-report.ru.
- ответить на контрольные вопросы: 1, 2, 3.

При изучении вопроса 2:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.compulenta.ru, www.isecurity.ru,www.oxpaha.ru, www.cyberterrorism-report.ru
- ответить на контрольные вопросы: 4,5.

При изучении вопроса 3:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.compulenta.ru, www.isecurity.ru,www.oxpaha.ru, www.cyberterrorism-report.ru.
- ответить на контрольные вопросы: 6, 7.

При изучении вопроса 4:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.compulenta.ru, www.isecurity.ru,www.oxpaha.ru, www.cyberterrorism-report.ru.
- ответить на контрольный вопрос: 8.

При изучении вопроса 5:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.compulenta.ru, www.isecurity.ru,www.oxpaha.ru, www.cyberterrorism report.ru.
- ответить на контрольный вопрос: 9.

Контрольные вопросы по теме

1. Чем обусловлены угрозы безопасности информации?
2. Перечислите пути реализации угроз информационной безопасности.
3. Как классифицируются угрозы безопасности информации по базовым признакам?
4. В чем заключается пассивное и активное проникновение в систему?
5. Как классифицируются каналы утечки конфиденциальной информации?
6. Как классифицируются удаленные атаки на интрасети?
7. Какие виды сетевых устройств являются объектами удаленных атак на интрасети?
8. Какие методы взлома интрасетей относятся к классическим и какие существуют?
9. Перечислите современные методы взлома интрасетей и объясните, как они используются?

При изучении темы необходимо:

- читать литературу:

1. «Информационная безопасность». Учебное пособие.
2. Герасименко В.А., Малюк А.А. «Основы защиты информации» - М.: АПО«Известия», 1997.
3. Мельников В.П. «Защита информации в компьютерных системах» - М.:«Финансы и статистика», 1997.
4. Милославская Н.Г., Толстой А.И. «Интрасети: доступ в Internet» - М.: Глава 1. -М: ООО «ЮНИТИ-ДАНА», 2000.
5. Проскурин В.Г., Крутов С.В. «Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах» - М.: «Радио и связь»,2000.
6. Белкин П.Ю. «Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных». - М.: «Радио и связь», 1999.

- посетить сайты: www.compulenta.ru, www.isecurity.ru, www.oxpaha.ru,www.cyberterrorism report.ru.

Форма представления отчета:

Студент должен продемонстрировать знание возможных угроз и слабо уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимое для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Предоставить отчет в письменном виде.

Практическое занятие № 2,3. Информационная безопасность в условиях функционирования в КР глобальных сетей.

Цель работы: Получение статистических знаний об атаках, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины.

Рекомендации к самостоятельной работе:
Повторить лекционный материал по теме «Информационная безопасность в условиях функционирования в России глобальных сетей».

Изучив тему, студент должен:

- уметь объяснить необходимость изучения информационной безопасности;
- знать статистику проявления компьютерных преступлений и наносимый ими ущерб;
- знать классификацию пользователей и злоумышленников в Internet;
- знать причины уязвимости Internet;
- знать основные понятия и определения, используемые при изучении информационной безопасности.

Изучая тему, необходимо акцентировать внимание на следующих понятиях:
безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, безопасность информации, аутентификация, верификация, идентификация.

Содержание работы:

Виды самостоятельной работы студентов:
- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Компьютерные преступления»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы
1. Что такое информационная безопасность?
2. Актуальность проблемы информационной безопасности.
3. Примеры взломов сетей и Web-узлов через Internet.
4. Пользователи и злоумышленники в Internet.
5. Причины уязвимости сети Internet.
6. Понятия и определения в информационной безопасности.

Методические указания по изучению вопросов темы

При изучении вопроса 1:
- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.hackzone.ru, www.megapolis.aaanet.ru,www.2600.com, www.cnews.ru, www.viruslist.com;
- принять участие в форуме по теме «Компьютерные преступления»;
- ответить на контрольные вопросы: 1,2.

При изучении вопроса 2:
- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы

- ссылки на ресурсы Интернет: www.hackzone.ru. www.megapolis.aaanet.ru.www.2600.com. www.enews.ru. www.viruslist.com;

- ответить на контрольные вопросы: 3, 4,5.

При изучении вопроса 3:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.hackzone.ru. www.megapolis.aaanet.ru.www.2600.com. www.enews.ru. www.viruslist.com;
- ответить на контрольный вопрос: 6.

При изучении вопроса 4:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.hackzone.ru. www.megapolis.aaanet.ru.www.2600.com. www.enews.ru. www.viruslist.com;
- ответить на контрольные вопросы: 7.8.

При изучении вопроса 5:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.hackzone.ru. www.megapolis.aaanet.ru.www-2600.com. www.enews.ru. www.viruslist.com;
- ответить на контрольный вопрос: 9.

При изучении вопроса 6:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.hackzone.ru. www.megapolis.aaanet.ru.www.2600.com. www.enews.ru. www.viruslist.com;
- ответить на контрольный вопрос: 10.

Контрольные вопросы по теме

1. Что такое информационная безопасность?
2. В чем заключается утечка информации?
3. Какова цель создания системы компьютерной безопасности?
4. Назовите виды компьютерных атак.
5. Откуда следует ожидать компьютерной атаки?
6. Приведите примеры взломов сетей и Web-узлов через Internet.
7. Перечислите и охарактеризуйте основных пользователей Internet.
8. Как классифицируются злоумышленники в Internet?
9. Какие факторы уязвимости Internet?
10. Дайте определения следующим понятиям: безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, целостность информации, аутентификация, верификация, идентификация.

При изучении темы необходимо:

- читать литературу:

1. «Информационная безопасность». Учебное пособие.
2. Герасименко В.А., Малюк А.А. «Основы защиты информации». Глава 1. -М.: «Известия», 1997.
3. Мельников В.И. «Защита информации в компьютерных системах». Раздел 1. - М.:«Финансы и статистика», 1997.
4. Милославская Н.Г., Толстой А.И. «Интрасети: доступ в Internet, защита». Глава 1. -М.: ООО «ЮНИТИ-ДАНА», 2000.
- посетить сайты: www.hackzone.ru, www.megapolis.ammet.ru, www.2600.com, www.cnews.ru, www.viruslist.com.

Форма представления отчета:

Студент должен изучить понятия: безопасность информации, угроза безопасности информации, несанкционированный доступ, нарушитель, злоумышленник, защита информации, целостность информации, аутентификация, верификация, идентификация. Предоставить отчет в письменном виде.

Практическое занятие № 4,5. Виды противников или «нарушителей». Понятие о видах вируса.

Цель работы: Получение знаний о существующих «компьютерных вирусах» и об алгоритмах их работы.

Рекомендации к самостоятельной работе:

Повторить лекционный материал по теме «Виды противников или «нарушителей». Понятие о видах вируса.».

Содержание работы:

Изучив тему, студент должен:

- знать, какие программы называются «компьютерными вирусами», чем они отличаются от других вредных программ;
- знать классификацию «компьютерных вирусов», и какую угрозу они представляют для безопасности информации;
- знать алгоритмы работы «компьютерных вирусов» и пути их проникновения в систему;
- уметь по индивидуальным признакам различать «компьютерные вирусы» различных классов;

Изучая тему, необходимо акцентировать внимание на следующих понятиях:

«компьютерные вирусы», свойства «компьютерных вирусов», вредные программы, резидентность, самошифрование, полиморфичность, «невидимка-вирусы», parasitig-вирусы, companion-вирусы, link-вирусы, файловые черви, макровирусы, сетевые вирусы, «троянские кони», логические бомбы.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;

- подготовка к участию в форуме по теме «Компьютерные вирусы»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Классификация «компьютерных вирусов».
2. Файловые вирусы.
3. Загрузочные вирусы.
4. Макровирусы.
5. Сетевые вирусы.
6. Вредные программы.

Методические указания по изучению вопросов темы

При изучении вопроса 1:

- читать учебное пособие «Информационная безопасность»;
- принять участие в форуме по теме «Компьютерные вирусы»
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.virusfist.com, www.subscribe.ru,www.refer.ru, www.virus.komi.ru.
- ответить на контрольные вопросы: 1, 2, 3.

При изучении вопроса 2:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.virusfist.com, www.subscribe.ru,www.refer.ru, www.virus.komi.ru
- ответить на контрольные вопросы: 4, 5, 6.

При изучении вопроса 3:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет' www.virusfist.com, www.subscribe.ru,www.refer.ru, www.virus.komi.ru.
- ответить на контрольные вопросы: 7, 8.

При изучении вопроса 4:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.virusfist.com, www.subscribe.ru,www.refer.ru, www.virus.komi.ru.
- ответить на контрольные вопросы: 9, 10.

При изучении вопроса 5 •

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.virusfist.com, www.subscribe.ru,www.refer.ru, www.virus.komi.ru.
- ответить на контрольный вопрос: 11.

При изучении вопроса 6:

- читать учебное пособие «Информационная безопасность»;

- изучить дополнительные материалы
  - ссылки на ресурсы Интернет: www.viruslist.com, www.subscribe.ru, www.refer.ru, www.virus.komi.ru.
- ответить на контрольный вопрос: 12.

Контрольные вопросы по теме

1. Какими основными свойствами обладают «компьютерные вирусы»?
2. По каким классам разделяются «компьютерные вирусы»?
3. Как классифицируются «компьютерные вирусы»?
4. Какие «компьютерные вирусы» относятся к файловым?
5. Как разделяются файловые «компьютерные вирусы» по способу размножения?
6. Объясните алгоритм работы файлового вируса.
7. Какие «компьютерные вирусы» относятся к загрузочным?
8. Объясните алгоритм работы загрузочного вируса.
9. Какие «компьютерные вирусы» относятся к макровирусам?
10. Объясните алгоритм работы макровируса.
11. Какие «компьютерные вирусы» относятся к сетевым?
12. Какие программы являются вредными и почему?

При изучении темы необходимо:

- читать литературу:

1. Касперский Е.В. «Компьютерные вирусы: что это такое и как с ними бороться». - М:«СК Пресс», 1998.
2. Фролов А.В., Фролов Г.В. «Осторожно: компьютерные вирусы». - М.: «Диалог-МИФИ», 1996.

- посетить сайты: www.viruslist.com, www.subscribe.ru, www.refer.ru,www.virus.komi.ru.

Форма представления отчета:

Студент должен изучить понятие сервиса безопасности, вопросы архитектурной безопасности, классификацию сервисов. Предоставить отчет в письменном виде.

Практическое занятие № 6,7.. Три вида возможных нарушений информационной системы. Защита.

Цель работы: Получение знаний о правилах защиты от «компьютерных вирусов». Знать основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы

Рекомендации к самостоятельной работе:

Повторить лекционный материал по теме «Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы».

Содержание работы:

Изучив тему, студент должен:

- знать, откуда проникают в компьютерную систему «компьютерные вирусы»;
- знать правила защиты от «компьютерных вирусов»;
- уметь выбрать антивирусную программу;

- уметь правильно использовать антивирусную программу;
- знать основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Изучая тему, необходимо акцентировать внимание на следующих понятиях: комплексный подход к информационной безопасности, законодательный уровень, государственная тайна, коммерческая тайна, лицензия, электронная цифровая подпись, нормативные документы.

Порядок изучения темы

Виды самостоятельной работы студентов:

- изучение учебного пособия «Информационная безопасность»;
- подготовка к участию в форуме по теме «Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы»;
- изучение дополнительной литературы;
- выполнение тестовых заданий по теме.

Вопросы темы

1. Законодательный уровень информационной безопасности.
2. Обзор российского законодательства.
3. Закон «Об информации, информатизации и защите информации».
4. О текущем состоянии российского законодательства.

Методические указания по изучению вопросов темы

При изучении вопроса 1:

- читать учебное пособие «Информационная безопасность»;
- принять участие в форуме по теме «Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы»;
- изучить дополнительные материалы
- ссылки на ресурсы Интернет: www.viruslist.com, www.subscribe.ru,www.new.russian.net.ru, www.dials.ru.
- ответить на контрольный вопрос: 1.

При изучении вопроса 2:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
- ссылки на ресурсы Интернет: www.viruslist.com, www.subscribe.ru,www.new.russian.net.ru, www.dials.ru.
- ответить на контрольный вопрос: 2.

При изучении вопроса 3:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы
- ссылки на ресурсы Интернет: www.viruslist.com, www.subscribe.ru,www.new.russian.net.ru, www.dials.ru.
- ответить на контрольные вопросы: 3,4, 5.

При изучении вопроса 4:

- читать учебное пособие «Информационная безопасность»;
- изучить дополнительные материалы

- ссылки на ресурсы Интернет: www.viruslist.com. www.subscribe.ru.www.new.russian.net.ru. www.dials.ru.
- ответить на контрольные вопросы: 6. 7.

Контрольные вопросы по теме

1. Что такое законодательный уровень ИБ?
2. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности.
3. Основные понятия закона «Об информации, информатизации и защите информации»
4. Другие законы и нормативные акты.
5. Обзор зарубежного законодательства в области ИБ.
6. Текущее состояние российского законодательства.
7. Стандарты в области информационной безопасности.

При изучении темы необходимо:

- читать литературу:

1. Касперский Е.В. «Компьютерные вирусы: что это такое и как с ними бороться». -ММ.: «СК Пресс». 1998.
2. Фролов А.В., Фролов Г.В. «Осторожно: компьютерные вирусы». - М.: «Диалог-МИФИ». 1996.

- посетить сайты: www.viruslist.com. www.subscribe.ru www.new.russian.net.ru.www.dials.ru.

Форма представления отчета:

Студент должен изучить понятие сервиса безопасности, знать основные нормативные руководящие документы. Предоставить отчет

Перевод 100 бальной рейтинговой оценки по дисциплине в традиционную четырех балльную

100-балльная система оценки	традиционная четырехбалльная система оценки
85-100 баллов	Оценка «отлично» / «зачтено»
70-84 баллов	Оценка «хорошо» / «зачтено»
50-69 баллов	Оценка «удовлетворительно» / «зачтено»
Менее 50 баллов	Оценка «неудовлетворительно» / «незачтено»

Формирование оценки по дисциплине с использованием балльно-рейтинговой системы работы студента[1]

Виды работы	Максимальное количество баллов
I,II модули	
Посещаемость	20
Текущий контроль	20
Творческий контроль	10
Промежуточная аттестация (тестирование)	50
Итого	100
Итоговая оценка	
СРС	50
Текущий контроль	50
Итого	100

7. Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. «Информационная безопасность». Учебное пособие.
2. Герасименко В.А., Малюк А.А. «Основы защиты информации». - М.: ИПО «Известия», 1997.
3. Мельников В.И. «Защита информации в компьютерных системах». - М.: Финансы и статистика», 1997.
4. Милославская Н.Г., Толстой А.И. «Интрасети: доступ в Internet». - М.: ООО«ЮНИТИ-ДАНА», 2000.
5. Проскурин В.Г., Крутов С.В. «Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах». - М.: Радио и связь».2000.
6. Белкин П.Ю. «Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных». - М.: «Радио и связь», 1999.
7. Касперский Е.В. «Компьютерные вирусы: что это такое и как с ними бороться». - М.:«СК Пресс», 1998.
8. Фролов А.В., Фролов Г.В. «Осторожно: компьютерные вирусы». - М.: «Диалог-МИФИ», 1996.
9. Горбатов В.С. Фатьянов А.А. «Правовые основы защиты информации». - М.: МИФИ.1999.

Дополнительная литература

10. *Законом КР от 22 июля 2016 года № 130* Об информатизации и электронном управлении
11. Закон Российской Федерации от 10.06.93 «О сертификации продукции и услуг»
12. Закон «О федеральных органах правительственной связи и информации»
13. Закон «О государственной тайне».
14. Постановление Правительства от 24.12.94 № 1418 «О лицензировании отдельных видов деятельности».
15. Закон «Об информации, информатизации и защите информации» от 20.02.95 № 24-ФЗ.
16. Постановление от 26.06.95 № 608 «О сертификации средств защиты информации».
17. Гостехкомиссия России. Руководящий документ. «Защита от несанкционированного доступа к информации. термины и определения».
18. Гостехкомиссия России. Руководящий документ. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа кинформации».
19. Гостехкомиссия России. Руководящий документ. «Средства вычислительной техники.Защита от несанкционированного доступа к информации. показатели защищенностиот несанкционированного доступа к информации».
20. Гостехкомиссия России. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
21. Гостехкомиссия России. Руководящий документ. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средствзащиты секретной информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».

Источники в INTERNET:

www.hackzone.ru;
www.megapolis.aaanet.ru;
www.2600.com;
www.cnews.ru;
www.viruslist.com;
www.compulenta.ru;
www.isecurity.ru;
www.oxpaha.ru;
www.cyberterrorism report.ru;
www.viruslist.com;
www.subscribe.ru;
www.refer.ru;
www.virus.komi.ru;
www.new.rassian.net.ru;
www.dials.ru;
www. sbcinfo/index.htm

Критерии оценивания знаний магистранта на экзамене с оценкой

От 85 до 100 баллов:

Обучающийся в полной мере владеет понятиями, фактами, теориями, методами, называет и дает определение, раскрывает объем понятий, их характеристику и содержание; имеет представление о возможных путях решения научных проблем; иллюстрирует проблему примерами. Ответ излагается четко, логично, аргументировано, с использованием научной терминологии.

От 70 до 84 баллов:

Обучающийся достаточно хорошо владеет понятиями, фактами, теориями, методами, при этом допускает небольшие неточности в определении понятий, установлении взаимосвязей; может, исходя из фактов, выделить существенные признаки объекта или явления. Ответ обоснованный, логично структурированный.

От 55 до 69 баллов:

Обучающийся демонстрирует пробелы в знании учебно-программного материала, недостаточно четко дает определение понятий. Ответ схематичный, имеют место речевые ошибки, нарушена логика изложения материала.

От 0 до 54 баллов:

Не владеет научными понятиями, представлениями по теме дисциплины; не может выделить существенные признаки объекта или явления. Ответ необоснованный, немотивированный, язык изложения скудный, неточный.

Итоговым контролем является экзамен с оценкой.

оценка	количество баллов
«отлично»	От 85 до 100 баллов
«хорошо»	От 70 до 84 баллов
«удовлетворительно»	От 55 до 69 баллов
«неудовлетворительно»	От 0 до 54 баллов