ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ УНИВЕРСИТЕТ

Составлен в соответствии с государственными требованиями к минимуму содержания и уровню подготовки выпускников по направлению 01.03.02 Прикладная математика и информатика и Положением «Об УМКД РАУ».

УТВЕРЖДАЮ:
д.ф.-м.н., профессор
Заведующий кафедрой
математической кибернетики
Арамян Рафик Грачикович
"08" августа 2020г.

Институт Математики и информатики

Кафедра: Математической кибернетики

Автор(ы): **к.т.н, и. о. доцента Ланина Н. С.**
Ученое звание, ученая степень, Ф.И.О

УЧЕБНАЯ ПРОГРАММА

Дисциплина: Б1.В.05 «Основы информационной безопасности»
Код и название дисциплины согласно учебному плану

Для бакалавриата:

Направление: 042.03.01 Реклама и связи с общественностью

Код и название специальности по ОКСО

Профиль: Реклама и связи с общественностью

ЕРЕВАН

1. Аннотация

В теоретической части курса рассматриваются основные понятия информационой безопасности в автоматизированных информационных системах, включая основные угрозы и средства защиты от них; рассматриваются вопросы криптографической защиты информации. В рамках дисциплины представлены вопросы безопасной информационно-аналитической работы в Internet; стеганографическая защита информации; основы цифровой защиты мультимедийной информации; опасности социальных сетей; интернет-мошенничество; специальные технические средства защиты.

Курс «Основы информационной безопасности» имеет непосредственную взаимосвязь с дисциплинами «Информатика» и учебного плана специальности «Реклама».

Студенты должны владеть основными разделами элементарной математики и информатики в объеме программы общеобразовательной школы.

Взаимосвязь дисциплины с другими дисциплинами учебного плана специальности (направления)

Дисциплина будет преподаваться во взаимосвязи с такими дициплинами как “Современные информационные технологии” и “ Компьютерные технологии и информатика ”

2. Цели и задачи дисциплины

Цель дисциплины: ознакомить студентов с основными понятиями информационной безопасности, включая основные угрозы и средства защиты от них; криптографическую защиту информации и специальные технические средства защиты, методами защиты персональных данных, авторского права на цифровой контент.

Задачи дисциплины: ознакомить студентов с основными понятиями информационной безопасности и научить криптографическим и стеганографическим методам защиты информации от несанкционированного доступа и использования.

3. Требования к уровню освоения содержания дисциплины (какие компетенции (знания, умения и навыки) должны быть сформированы у студента ПОСЛЕ прохождения данной дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- готовностью к кооперации с коллегами, работе в коллективе (ОК-3);
- способностью находить организационно-управленческие решения в нестандартных ситуациях и готов нести за них ответственность (ОК-4);

- владением основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией (ОК-12);

После прохождения дисциплины студент должен:

Знать: основные понятия информационной безопасности, включая основные угрозы и средства защиты от них.

Уметь: защищать свою информацию от несанкционированного доступа и использования

Владеть: основными методами информационной безопасности для решения практических задач.

4. Трудоемкость дисциплины и виды учебной работы по учебному плану

Курс «Особенности информационной безопасности» рассчитан на 1 семестр по 36 аудиторных часов. Курс изучается в форме лекционных и практических занятий. В конце студенты сдают зачет.

Виды учебной работы	Всего, в акад. часах
1. **Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:**	**72**
1.1. Аудиторные занятия, в т. ч.:	**36**
1.1.1. Лекции	
1.1.2. Практические занятия, в т. ч.	**36**
1.1.2.1. Обсуждение прикладных проектов	
1.1.2.2. Кейсы	
1.1.2.3. Деловые игры, тренинги	
1.1.2.4. Контрольные работы	**3**
1.1.2.5. Другое (указать)	
1.1.3. Семинары	
1.1.4. Лабораторные работы	
1.1.5. Другие виды (указать)	
1.2. Самостоятельная работа, в т. ч.:	**36**
1.2.1. Подготовка к экзаменам	
1.2.2. Другие виды самостоятельной работы, в т.ч. (указать)	
1.2.2.1. Письменные домашние задания	
1.2.2.2. Курсовые работы	
1.2.2.3. Эссе и рефераты	
1.2.2.4. Другое (указать)	
1.3. Консультации	
1.4. Другие методы и формы занятий	
Итоговый контроль (экзамен, зачет, диф. зачет - указать)	**зачет**

5. Содержание дисциплины

5.1. Распределение объема дисциплины по темам и видам учебной работы

Разделы и темы дисциплины	Всего (ак. часов)	Лекции(ак. часов)	Практ. занятия (ак. часов)	Семина-ры (ак. часов)	Лабор. (ак. часов)	Др. виды занятий (ак. часов)
1		3	4	5	6	7
Тема 1. Актуальность проблемы информационной безопасности	**1**	**1**				
Тема 2. Система информационной безопасности	**1**	**1**				
Тема 3.Проблемы идентификации пользователей и аутентификации данных	**6**	**2**	**4**			
Тема 4. Криптографическое закрытие информации	**12**	**4**	**8**			
Тема 5.Стеганографическая защита информации	**10**	**4**	**6**			
Тема 6. Подслушивание. Электронная разведка	**2**	**2**				
Тема 7. Интернет-мошенничество	**4**	**4**				
ИТОГО	**36**	**18**	**18**			

5.2. Содержание разделов и тем дисциплины:

Тема 1. Актуальность проблемы информационной безопасности

Понятие информации. Классификация. Определение информационной безопасности. Понятие угрозы. Основные угрозы информационной безопасности. Классификация угроз.

Тема 2. Система информационной безопасности

Средства обеспечения информационной безопасности. Система информационной безопасности. Основные принципы построения системы информационной безопасности.

Тема 3. Проблемы идентификации пользователей и аутентификации данных

Универсальные механизмы обеспечения сетевой информационной безопасности. Идентификация и проверка подлинности пользователей компьютерных сетей. Аутентификация и авторизация. Контроль доступа.

Тема 4. Криптографическое закрытие информации

Криптология. Основные определения и примеры. Традиционные криптографические методы закрытия информации. Электронная цифровая подпись. Электронное правительство.

Тема 5.Стеганографическая защита информации

Стеганография: определение, примеры, назначение. Отличие стеганографии от криптографии. ЦВЗ-технологии, области применения. Защит а авторского права на цифровой контент.

Тема 6. Интернет-мошенничество

Актуальность проблемы интернет-мошенничества. Виды интернет-мошенничества. Основные признаки мошенничества. Защита от интернет-мошенничества. Опасности социальных сетей.

5.3. Краткое содержание семинарских/практических занятий

Название тем	Количество часов
Тема 1. Работа в локальной компьютерной сети. Установка пароля.	**2**
Тема 2. Создание зашифрованных сообщений и обмен ими в локальной сети с помощью коммуникационной программы LAN Messenger	**2**
Тема 3. Освоение системы PGP (создание зашифрованных сообщений, постановка и верификация ЭЦП)	**4**
Тема 4. Тестовые испытания на стенде информационной безопасности	**6**
Тема 5. Освоение стеганографической программы S-tools маскировка сообщений в аудио файлы. Маскировка сообщений в изображениях	**4**

5.4. Экзаменационные (и или зачетные) вопросы

1. Постановка проблемы информационной безопасности. Понятие информации, определение. Конфиденциальная информация. Классификация информации.
2. Определение информационной безопасности. Доступность, целостность, конфиденциальность. Угрозы, классификация.
3. Основные средства обеспечения информационной безопасности. Система информационной безопасности.
4. Основные принципы построения системы информационной безопасности.
5. Универсальные механизмы обеспечения информационной безопасности.
6. Криптология. Основные определения и примеры.
7. Основные методы криптографического закрытия информации.
9. Электронная цифровая подпись. Назначение. Области применения
10. Стеганографическая защита информации. Основные сведения и примеры. Отличие стеганографии от криптографии.
11. Цифровые водяные знаки. Назначение, сферы применения ЦВЗ-технологий.
13. Подслушивание. Электронная разведка. Специальные технические средства информационной безопасности.
16. Интернет-мошенничество. Фишинг. Опасность социальных сетей.
17. Термины ГЛОССАРИЯ

6. Учебно-методическое обеспечение дисциплины

6.1. Методические рекомендации по изучению дисциплины для студентов

Рабочей программой дисциплины предусмотрена самостоятельная работа студентов в объеме 36 часов. Самостоятельная работа проводится с целью углубления знаний по дисциплине и предусматривает:

- изучение и усвоение лекционного (теоретического) материала,
- подготовку к контрольной работе,
- изучение дополнительной литературы,
- подготовку к практическим занятиям;
- работу с Интернет-ресурсами;
- подготовку к модулю и зачету.

6.2. Рекомендуемая литература:

а) Базовый учебник

1.Таирян В.И. «Основы информационной безопасности», Ереван, РАУ, 2007

2.Герасименко В.А. «Защита информации в автоматизированных системах обработки данных», М., 1994

б) Основная литература

1. Д.Г. Асатрян, Н.С. Асатрян, Н.С. Ланина, С.В. Таирян Учебно-методическое пособие «Основы цифровой защиты мультимедийной информации», Ереван, РАУ, 2011

2. Э. Таненбаум «Компьютерные сети» 4.е изд. СПб, 2006

3. Коханович Г. Ф., Пузыренко А. Ю. «Компьютерная стеганография. Теория и практика», Киев, 2006

в) Дополнительная литература

1. Р. Гонсалес, Р. Вудс Цифровая обработка изображений, Москва, Техносфера, 2006

2. Барсуков В. С., Романцов А. П. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века. Специальная техника № 4-5 1998 г. http://www.ess.ru/publications/articles/steganos/steganos.htm

3. Таирян В. И. О доктрине информационно-психологического пояса безопасности электронного правительства Республики Армения Международная научно-практическая конференция «Вопросы безопасности информационнх систем», Ереван, 2008.

4. Ланина Н. С. Об устойчивости к атакам пространственного алгоритма встраивания в изображение цифровых водяных знаков. Тезисы докладов научно-практической конференции по вопросам надежности и безопасности информационных систем. Армянская технологическая академия Майкрософт АРЭЙ. Ереван, с. 26-29, 2007.