МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ, КУЛЬТУРЫ И СПОРТА РА

ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ УНИВЕРСИТЕТ

Составлена в соответствии с федеральными Государственными требованиями к структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура)

УТВЕРЖДАЮ:
Проректор по науке
_____ П.С. Аветисян
«21» июня 2024г.

Институт: Математики и Информатики
Кафедра: Математической кибернетики

Учебная программа подготовки аспиранта и соискателя
ДИСЦИПЛИНА: 2.1.1 Кибербезопасность в облачной среде

2.3.6. Методы и системы защиты информации, информационная безопасность
-Шифр *наименование научной специальности*

Программа одобрена на заседании кафедры протокол № 18 от 11.06.2024 г.

Утверждена Ученым Советом ИМИ протокол № 13 от 14.06.2024г.

Заведующий кафедрой _____ д.ф.м.н., профессор Арамян Р.Г.
Подпись *И.О.Ф, ученая степень, звание*

Разработчик программы _____ к.ф.м.н., Абраамян С.Е.
Подпись *И.О.Ф, ученая степень, звание*

Ереван 2024

Общие положения

Настоящая рабочая программа обязательной дисциплины (модуля) **«Кибербезопасность в облачной среде»** образовательной программы послевузовского профессионального образования (ОП ППО) ориентирована на аспирантов университета, уже прослушавших общие и специальные курсы по защите информации от ВПО, теории кодирования, теории информации, введению в информационную безопасность.

1. Цели изучения дисциплины (модуля)

Целью изучения дисциплины **«Кибербезопасность в облачной среде»** является получение навыков использования основных методов и систем защиты информации в вычислительных сетях.

Место дисциплины в структуре основной профессиональной образовательной программы послевузовского профессионального образования (аспирантура).

2. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

Аспирант должен

- Знать:

- научные принципы обеспечения комплексной защиты информации на основе существующих программ и методик
- основные угрозы информации в информационных системах
- характерные взаимосвязи и взаимозависимости развития методов, способов и средств защиты информации как проявление объективных закономерностей эволюции в области информационной безопасности
- существующие методы и средства, применяемые для контроля и защиты информации
- системные вопросы защиты программ и данных
- требования к защите автоматизированных систем от НСД
- представлениями о новых схемах аппаратуры контроля и средствах автоматизации контроля

- Уметь:

– анализировать методы и средства контроля и защиты информации и разрабатывать предложения по их совершенствованию и повышению эффективности ЗИ

- Владеть:

– навыками пользования действующими нормативными и методическими документами в области информационной безопасности и защиты информации
– навыками обобщения результатов исследований, полученных отечественными и зарубежными исследователями в области информационной безопасности
– методами планирования проведения научного исследования и совокупностью способов

3. Объем дисциплины (модуля) и количество учебных часов

4. Вид учебной работы	**Кол-во зачетных единиц*/уч.часов**
Аудиторные занятия	
Лекции (минимальный объем теоретических знаний)	8
Семинар	18
Практические занятия	-
Другие виды учебной работы (авторский курс, учитывающий результаты исследований научных школ Университета, в т.ч. региональных)	-
Формы текущего контроля успеваемости аспирантов	-
Внеаудиторные занятия:	
Самостоятельная работа аспиранта	10
ИТОГО	36
Вид итогового контроля	Составляющая экзамена кандидатского минимума **зачет**

5. Содержание дисциплины (модуля)

4.1 Содержание лекционных занятий

№ п/п	Содержание	Кол-во уч.часов
1	Помехоустойчивое кодирование	1
2	Основы криптографии	2
3	Основы стеганографии	2
4	Основы цифровой защиты информации	3

Всего:	**8**

4.2 Практические занятия

Практические занятия не предусмотрены учебным планом

4.3 Другие виды учебной работы

Другие виды учебной работы не предусмотрены учебным планом.

4.4 Самостоятельная работа аспиранта

№ п/п	Виды самостоятельной работы	Кол-во уч.часов
1	Подготовка научного реферата по теме дисциплины	28
Всего:		**28**

5 Перечень контрольных мероприятий и вопросы к экзаменам кандидатского минимума

1 Определение и основные понятия систем защиты информации (СЗИ). Общеметодологические принципы построения СЗИ, их сущность и содержание.
2 Основы архитектурного построения СЗИ. Функциональная, организационная и структурная модели СЗИ. Ядро СЗИ, его функции и состав.
3 Типизация и стандартизация архитектурного построения СЗИ. Функциональная, организационная и структурная модели СЗИ. Ядро СЗИ, его функция и состав.
4 Типизация и стандартизация архитектурного построения СЗИ. Уровни типизации. Типовые СЗИ, их состав и общее содержание. Типовые функциональные и структурные подсистемы СЗИ. Типовые проектные решения компонентов СЗИ.
5 Основы методологии проектирования СЗИ. Классификация и анализ постановок задач проектирования СЗИ. Методика выбора требований к защите информации.
6 Методика создания СЗИ на основе типовых проектных решений. Методика выбора и привязки типовой СЗИ. Методика проектирования СЗИ на базе типовых подсистем и компонентов.
7 Методика проектирования индивидуальных (уникальных) СЗИ. Условия, в которых необходимо или целесообразно создание уникальных СЗИ. Последовательность и общее содержание проектирования. Методы определения требуемых вероятностей надежного осуществления функций полного их множества. Методика оптимального выбора задач, необходимых для осуществления функций защиты. Методика выбора средств защиты, необходимых и достаточных для эффективного решения выбранных средств защиты. Методика объединения выбранных средств в СЗИ. Технико-экономические оценки проекта.
8 Организация процесса создания СЗИ. Последовательность и содержание обследования объекта, для которого создается СЗИ. Организация непосредственного проектирования, монтажа, наладки и испытаний СЗИ. Информационное обеспечениепроектирования.

6 Образовательные технологии

В процессе обучения применяются следующие образовательные технологии:

1. Сопровождение лекций показом визуального материала.

2. Проведение лекций с использованием интерактивных методов обучения.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

Учебно-методические и библиотечно-информационные ресурсы обеспечивают учебный процесс и гарантируют качественное освоение аспирантом образовательной программы. Университет располагает обширной библиотекой, включающей научную литературу, научные журналы и труды научно-практических конференций по основополагающим проблемам науки.

7.1. Основная литература:

1) Ященко В.В. Введение в криптографию. М., 2001
2) Гене О.В. Основные положения стеганографии. М., 2000
3) Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М., 2002
4) Мелик-Шахназаров Б.Б. Информационнпые основы теории управления. Ереван, РАУ, 2003

7.2. Дополнительная литература

1) Геолецян Г.Г. Структурная и топологическая оптимизация систем автоматизации. Ереван, РАУ, 2007
2) Таирян В.И. Введение в алгебраическую теорию кодирования. Ереван, РАУ, 2003
3) Таирян В.И. Основы информационной безопасности в компьютерных сетях. Ереван, РАУ, 2006
4) Таирян В.И., Таирян С.В., Берберян Л.С. Обеспечение информационно-психологической безопасности методами социальной инженерии и стеганографии. Ереван, РАУ, 2010
5) Авторский коллектив, рук. Таирян В.И. Экспертные методы в задачах информационно-психологической безопасности систем. Ереван, «ВАН АРЬЯН», 2011
6) Авторский коллектив, рук. Таирян В.И. Математические и практические основы обеспечения информационной безопасности. Ереван, 2010
7) Таирян В.И., Таирян С.В., Абрамян А.А., Таирян М.В. Управление информационно-психологической безопасностью банковских систем. Ереван, РАУ, 2011
8) Асатрян Д.Г., Асатрян Н.С., Ланина Н.С. Таирян С.В.. Основы цифровой защиты информации.

7.3. Интернет-ресурсы

1) http://www.mathnet.ru/

8 Материально-техническое обеспечение

Кафедра математической кибернетии располагает материально-технической базой, обеспечивающей проведение теоретической и практической подготовки, предусмотренных учебным планом аспиранта в специализированной компьютерной аудитории.