

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ, КУЛЬТУРЫ И СПОРТА РА
ГООУ 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

« 19 » 07 2023г.



Институт: Математики и Информатики
Кафедра: Математической кибернетики

Учебная программа подготовки аспиранта и соискателя
ДИСЦИПЛИНА: 2.1.8.1

Модели и методы управления информационной безопасностью
наименование дисциплины (модуля) по учебному плану подготовки аспиранта

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

Программа одобрена на заседании
кафедры
Утверждена Ученым Советом ИМИ

протокол № 14 от 17.07.2023 г.
протокол № 15 от 18.07.2023г.

Заведующий кафедрой


Подпись

д.ф.м.н., профессор Арамян Р.Г.
И.О.Ф, ученая степень, звание

Разработчик программы


Подпись

к.т.н., Таирян С.В.
И.О.Ф, ученая степень, звание

Ереван 2023

Общие положения

Настоящая рабочая программа обязательной дисциплины (модуля) «**Модели и методы управления информационной безопасностью**» образовательной программы послевузовского профессионального образования (ОП ППО) ориентирована на аспирантов университета, уже прослушавших общие и специальные курсы по введению в информационную безопасность, теории информации.

1. Цели изучения дисциплины (модуля)

Целью изучения дисциплины «**Модели и методы управления информационной безопасностью**» является получение навыков применения основных моделей и методов управления информационной безопасностью 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:

- основные понятия, термины, определения в бизнес-процессах, а также понятия анализа видов информации, в которых данные процессы проявляются: учредительная и лицензионная база организации, правовая сфера бизнеса, внутренняя нормативная база организации, внешняя и внутренняя отчетность, материальные и информационные активы
- основные методики оценки уровня информационной безопасности организации и примеры их использования
- основные методы противодействия «внутренним» угрозам информационной безопасности организации
- архитектуру основных стандартов защиты информации

- Уметь:

- использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации, методы противодействия «внутренним» угрозам информационной безопасности организации, методы анализа рисков информационной безопасности, методы

организационного проектирования, методы управления информационными активами организации

- Владеть:

- навыками использования методов изучения структуры современной коммерческой организации и подходов к управлению службой защиты информации как систематической практической деятельности коллегиальных органов управления организацией и руководителя службы, направленной на формирование и поддержание концептуальных и организационных основ деятельности организации и эффективное выполнение поставленных задач

3. Объем дисциплины (модуля) и количество учебных часов

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

4. Содержание дисциплины (модуля)

4.1 Содержание лекционных занятий

№ п/п	Содержание	Кол-во уч. часов
1	Основные понятия и определения информационной безопасности	2
2	Практические подмодули с методическими инструкциями.	2

3	Криптографические протоколы.	2
4	Аудит информационной безопасности систем. Построение карты сети. Очистка и проверка системы. Прослушивание трафика сети.	2
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. Необходимость, сущность и основные понятия управления защитой информации. Особенности управления на государственном, региональном (ведомственном) и объектовом уровнях. Особенности управления защитой в автоматизированных системах обработки данных.
2. Структура системы органов, ответственных за защиту информации. Основные функции органов государственного, регионального (ведомственного) и объектового уровней
3. Основные положения концепции центров защиты информации (ЦЗИ). Назначение и организационно-правовой статус ЦЗИ. Основные функции ЦЗИ. Перечень и содержание услуг, оказываемых ЦЗИ своим абонентам. Примерная структура ЦЗИ. Организация работы ЦЗИ
4. Служба защиты информации (безопасности) на объекте. Назначение и организационно-правовой статус службы. Функции и задачи службы, способы и методы их решения. Примерная организационная структура службы. Использование средств ЭВТ в работе службы
5. Технология управления функционированием СЗИ. Общая технологическая схема управления. Методы и технология планирования работы СЗИ. Организация и технологическая схема оперативно-диспетчерского регулирования процессов функционирования СЗИ. Организация и

содержание календарно-планового руководства защитой. Организация и содержание обеспечения повседневной деятельности службы защиты (безопасности). Технология аналитико-синтетической обработки данных о работе СЗИ.

6. Социально-психологические аспекты защиты информации. Требования к физическому, морально-этическому и психоэмоциональному состоянию работников органов защиты информации. Способы и методы подбора кадров органов защиты. Организация обучения и воспитания кадров. Способы и методы организации работы коллективов органов защиты и поддержания в них требуемого морально-психологического климата

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. Яценко 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. Шнайер Б. Прикладная криптография. М.: Триумф, 2002
5. Мелик-Шахназаров Б.Б. Информационные основы теории управления. Ереван, РАУ, 2003
- 6.

7.2. Дополнительная литература

1. Таирян В.И. Основы информационной безопасности в компьютерных сетях. Ереван, РАУ, 2006

2. Таирян В.И., Таирян С.В., Берберян Л.С. Обеспечение информационно-психологической безопасности методами социальной инженерии и стеганографии. Ереван, РАУ, 2010
3. Авторский коллектив, рук. Таирян В.И. Экспертные методы в задачах информационно-психологической безопасности систем. Ереван, «ВАН АРЬЯН», 2011
4. Авторский коллектив, рук. Таирян В.И. Математические и практические основы обеспечения информационной безопасности. Ереван, 2010
5. Таирян В.И., Таирян С.В., Абрамян А.А., Таирян М.В. Управление информационно-психологической безопасностью банковских систем. Ереван, РАУ, 2011

7.3. Интернет-ресурсы

1. <http://www.mathnet.ru/>

8 Материально-техническое обеспечение

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