ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

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

УТВЕРЖДАЮ:
Директор института:
Калашян М.А.
"23" июня 2022 г.
Зав. кафедрой
Саркисян О.Л.

Институт: Права и Политики

Кафедра: Политологии

Автор(ы): преподаватель Оганесян Т.Г.

УЧЕБНАЯ ПРОГРАММА

Дисциплина: Б1.О.11 Информационная безопасность

Магистерская программа: «Национальная безопасность»

Направление: 41.04.04 Политология

Форма обучения: очно-заочная

ЕРЕВАН

Структура и содержание УМКД

1. **Титульный лист**
2. **Перечень и структура элементов, составляющих УМКД**
3. **Аннотация**

3.1. Краткое описание содержания данной дисциплины;

Данный курс предполагает освещение и анализ важнейшей составляющей современной системы национальной безопасности – информационной безопасности. Раскрываются сущность и особенности информационного пространства. Понятие информационные войны: сущность, история, методологические основания, модели. Информационное оружие как основное средство ведения информационной войны. Методы сбора и анализа информации. Базовые знания об информационном противостоянии и методах психологического давления на общества противоборствующих сторон. Основные типы угроз кибербезопасности и практические знания по защите целостности и доступности информации. Применение полученных знаний с целью правильного проведения анализа угроз информационной безопасности.

Курс «Информационная безопасность» тесно взаимосвязан с такими дисциплинами как «Компьютерные технологии в политических науках», «Основы национальной безопасности», «Медиа-планирование и медиа-анализ», «Проблемы региональной безопасности» и др..

3.2. Требования к исходным уровням знаний и умений студентов для прохождения дисциплины

Студент должен иметь базовые знания по теоретическим разделам своей специальности и достаточную общеобразовательную подготовку по гуманитарным наукам, в частности, по сбору и анализу информации, понятия основных концепций национальной безопасности.

4. **Учебная программа**

4.1. Цели и задачи дисциплины

Цель преподавания дисциплины – выработать целостные представления об информационной безопасности и ее месте в системе национальной безопасности государств на примере Нагорно-Карабахского конфликта.

Задачами изучения дисциплины являются:

- Выявить и определить сущность и содержание актуальных проблем теории и практики обеспечения информационной безопасности,
- Раскрыть роль информационной безопасности в системе национальной безопасности государства и безопасности общества,
- Приобрести навыки сбора и анализа информации, выявления методов информационного воздействия.

4.2. Требования к уровню освоения содержания дисциплины

В результате изучения дисциплины студент должен

знать:

- Терминологию в области информационной безопасности,
- методы и средства обеспечения информационной безопасности,
- методы нарушения конфиденциальности, целостности и доступности информации,
- методы сбора и анализа информации,
- методы и технологии проверки достоверности сведений (факт-чекинг).

уметь:

- Правильно проводить анализ угроз информационной безопасности,
- применять на практике основные общеметодологические принципы теории информационной безопасности,
- провести контент-анализ, выявить факты и определить основную цель/цели распространения данной информации,
- выработать сценарии и практические шаги противодействия и нейтрализации последствий информационных атак.

4.3. Трудоемкость дисциплины и виды учебной работы (в академических часах и зачетных единицах) (см. приложение 1)
  4.3.1. Объем дисциплины и виды учебной работы
  4.3.2. Распределение объема дисциплины по темам и видам учебной работы
4.4. Содержание дисциплины (см. приложение 2)
  4.4.1. Разделы дисциплины с указанием видов занятий (лекции, семинарские и практические занятий, лабораторные работы) и их трудоёмкость в академических часах и зачетных единицах
  4.4.2. Краткое содержание разделов дисциплины в виде тематического плана
  4.4.3. Краткое содержание семинарских/практических занятий и лабораторного практикума**
4.5. Материально-техническое обеспечение дисциплины
4.6. Модульная структура дисциплины с распределением весов по формам контролей (см. приложение 3)
4.7. Формы и содержание текущего, промежуточного и итогового контролей

5. Теоретический блок

5.1. Материалы по теоретической части курса[1]
  5.1.1. Учебник(и)*

- Информационная война. Проблемы и модели, Расторгуев, Сергей Павлович, 2006г.
- Основы информационной безопасности, Расторгуев, Сергей Павлович, 2007г.

  5.1.2. Учебное(ые) пособие(я)*

Информационные войны: история и современность, учебное пособие для студентов высших учебных заведений, Сулейманова Ш.С., Назарова Е.А., 2017 г.

  5.1.3. Курс лекций*
  5.1.4. Краткие конспекты лекций*

[1] Должен быть хотя бы один вид материалов, из числа указанных в п.п. 5.1.1.-5.1.5.

5.1.5. Электронные материалы (электронные учебники, учебные пособия, курсы и краткие конспекты лекций, презентации PPT и т.п.)[2]

Презентации (PPTX):

- Информационная война: основные понятия
- Методы сбора и анализа информации: работа с поисковыми системами

5.2. Глоссарий/терминологический словарь*

6. Практический блок

6.1. Планы практических и семинарских занятий**

6.2. Планы лабораторных работ и практикумов**

6.3. Материалы по практической части курса[3]

6.3.1. Учебно-методические пособия *

6.3.2. Учебные справочники*

- Информационная безопасность: стандартизированные термины и понятия, Парошин А.А., 2010 г.
- Информационная безопасность, Ярочкин И.В., 2004 г.

6.3.3. Задачники (практикумы)*

6.3.4. Хрестоматии*

6.3.5. Наглядно-иллюстративные материалы*

Презентации (PPTX):

- Информационная война: основные понятия
- Методы сбора и анализа информации: работа с поисковыми системами

7. Блок ОДС и КИМ

7.1. Вопросы и задания для самостоятельной работы студентов

Вопросы:

1. Виды информации, её свойства и особенности их взаимодействия.
2. Перечислить свойства защищенной информации, выявить конкретные нарушения свойства согласно задаче.
3. Какие угрозы безопасности информации являются преднамеренными?
4. Укажите перечень грифов секретности для носителей сведений, составляющих государственную тайну (согласно законодательству РФ и Республики Армения).
5. Доктрина информационной безопасности.
6. Причины и источники угроз национальным интересам страны.
7. Важнейшие нормативные правовые акты, касающиеся информационной безопасности.
8. Информация и право. Информация как объект правового регулирования.
9. Указать правильный порядок процесса регистрации пользователя в системе.

[2] Должен быть хотя бы один вид электронных материалов, указанных в п. 5.1.5.

[3] В данном разделе должен быть хотя бы один вид материалов, из числа указанных в п.п. 6.3.1-6.3.5.

10. Какие методы аутентификации существуют? Как минимизировать угрозы безопасности учетных данных?
11. Что такое недостоверная информация?
12. Информационная война, методы и средства её ведения
13. Информационное оружие, его классификация и возможности
14. Причины, виды, каналы утечки и искажения информации
15. Методы нарушения конфиденциальности, целостности и доступности информации

Задачи:

1. Провести сбор и анализ данных по заданной тематике,
2. Выполнить задачи по обеспечению базового уровня информационной безопасности,
3. Используя шифр Цезаря, определить зашифрованное слово.
4. Найти источник/и информации, проверить достоверность.

7.2. Тематика курсовых, рефератов, эссе и других форм самостоятельных работ**
7.3. Образцы вариантов контрольных работ, тестов и/или других форм текущих и промежуточных контролей**
7.4. Перечень экзаменационных вопросов**

1. Виды информации, её свойства и особенности их взаимодействия.
2. Перечислить свойства защищенной информации, выявить конкретные нарушения свойства согласно задаче.
3. Какие угрозы безопасности информации являются преднамеренными?
4. Укажите перечень грифов секретности для носителей сведений, составляющих государственную тайну (согласно законодательству РФ и Республики Армения).
5. Доктрина информационной безопасности.
6. Причины и источники угроз национальным интересам страны.
7. Важнейшие нормативные правовые акты, касающиеся информационной безопасности.
8. Информация и право. Информация как объект правового регулирования.
9. Указать правильный порядок процесса регистрации пользователя в системе.
10. Какие методы аутентификации существуют? Как минимизировать угрозы безопасности учетных данных?
11. Что такое недостоверная информация?
12. Информационная война, методы и средства её ведения
13. Информационное оружие, его классификация и возможности
14. Причины, виды, каналы утечки и искажения информации
15. Методы нарушения конфиденциальности, целостности и доступности информации
16. Провести сбор и анализ данных по заданной тематике,
17. Выполнить задачи по обеспечению базового уровня информационной безопасности,
18. Используя шифр Цезаря, определить зашифрованное слово.
19. Найти источник/и информации, проверить достоверность.

Приложение 1.

Таблица трудоемкости дисциплин и видов учебной работы

Виды учебной работы	Всего, в акад. часах	Распределение по семестрам					
		___ сем	___ сем	___ сем	___ сем.	___ сем	____ сем.
1	2	3	4	5	6	7	8
1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:	**108**						
1.1. Аудиторные занятия, в т. ч.:	**18**						
1.1.1. Лекции	**10**						
1.1.2. Практические занятия, в т. ч.	**8**						
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	**36**						
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.:	**54**						
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)							

Приложение 2.

Содержание дисциплин

Форма 1. Тематический план и трудоемкость аудиторных занятий (модули, разделы дисциплины и виды занятий) по учебному плану

Разделы и темы дисциплины	Всего (ак. часов)	Лекции (ак. часов)	Практ. Занятия (ак. часов)	Семина-ры (ак. часов)	Лабор. (ак. часов)	Другие виды занятий (ак. часов)
1	**2=3+4+5+6 +7**	**3**	**4**	**5**	**6**	**7**
Модуль 1. Основы информационной безопасности						
Введение						
Раздел 1. Общие проблемы информационной безопасности	**4**	**2**	**2**			
Тема 1.1. Понятие информации и информационной безопасности						
Тема 1.2. Методы нарушения конфиденциальности, целостности и доступности информации.						
Раздел 2. Проверка достоверности информации						
Тема 2.1. Методы и инструменты проверки достоверности информации (Фактчекинг)	**4**	**2**	**2**			
Модуль 2. Информационная безопасность в системе национальной безопасности РА и РФ:						
Раздел 2. Проблемы информационной безопасности в РА и РФ						

Тема 2.1. Основы государственной политики РА и РФ в области информационной безопасности (ИБ):	**4**	**2**	**2**			
Тема 2.2. Виды и источники угроз национальной безопасности РА и РФ.						
Модуль 3. Информационная война						
Тема 3.1. Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство.	**6**	**4**	**2**			
Тема 3.2. Информационное оружие, его классификация и возможности.						
ИТОГО	**18**	**10**	**8**			

Форма 2. Содержание разделов и тем дисциплины
Модуль 1

Введение
Основы информационной безопасности

Особенность нынешнего периода — частичный переход к информационному общество, где информация становится важным ресурсом не только для общения, но и конструирования внешне- и внутригосударственной политики. Безопасность информации является одним из важнейших факторов обеспечения национальной, в том числе. и государственной безопасности. Изучение дисциплины «Информационная безопасность» позволяет будущему специалисту — политологу приобрести знания о видах информации, освоить методы сбора и анализа информации, получить базовые знания об информационном противостоянии и методах психологического давления на общества противоборствующих сторон, изучить основные типы угроз в сфере кибербезопасности и получить практические знания по защите целостности и доступности информации, применить полученные знания с целью правильного проведения анализа угроз информационной безопасности.

Цель преподавания дисциплины – выработать целостные представления об информационной безопасности и ее месте в системе национальной безопасности государств.

- Информационная безопасность, Ярочкин В. И., Учебник для вузов, Академический Проект; Гаудеамус, 2-е изд.— 2004, сс. 6-30.
- Информационная безопасность, Партыка Т.Л., Попов И.И., Москва 2010, сс. 10-29.

Раздел 1. Общие проблемы информационной безопасности

Тема 1.1. Понятие информации и информационной безопасности

Под информационной безопасностью подразумевается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

- Информационная Безопасность, Макаренко С.И., Ставрополь 2009, сс. 20-32,
- Информационная безопасность, Ярочкин В. И., Учебник для вузов, Академический Проект; Гаудеамус, 2-е изд.— 2004, сс. 6-30.
- Информационная безопасность, Партыка Т.Л., Попов И.И., Москва 2010, сс. 10-29.

Тема 1.2. Методы нарушения конфиденциальности, целостности и доступности информации.

На сегодняшний день сформулировано три базовых принципа,
которые должна обеспечивать информационная безопасность:

- целостность данных — защита от сбоев, ведущих к потере
- информации, а также защита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей

- Информационная безопасность, Партыка Т.Л., Попов И.И., Москва 2010, сс. 10-52.

Раздел 2. Проверка достоверности информации

Искаженная целиком или полностью информация иногда распространяется в медиа преднамеренно и служит пропагандистским или манипуляционным целям. Информация может искажаться также вследствие ошибки при переводе, использовании синонимов, отсутствия отсылки к первоисточнику, частичной передачи сообщения, вырывания из контекста, изложения собственными словами и др. То есть происходит трансформация содержания, которая может привести к искажению первичного смысла.

В словаре Merriam-Webster слово «дезинформация» определяется как распространение преднамеренной, зачастую тайной, ложной информации с целью оказания воздействия на сознание общества, сокрытия истины, а Оксфордский словарь определяет этот термин как адресованные правительственными органами конкурентам или средствам массовой информации сведения, нацеленные на введение в заблуждение.

- Fake News, Дезинформация в медиа, Муратова Н., Тошпулатова Н., Алимова Г., Ташкент 2020,

- Journalism, 'Fake News' & Disinformation, Handbook for Journalism Education and Training, Berger G., UNESCO 2018,
- Искажение информации: пропаганда или ошибка?, Г. Григорян, Аналитический Центр Орбели, 2019 г.

Тема 2.1. Методы и инструменты проверки достоверности информации (Фактчекинг)

Модуль 2. Информационная безопасность в системе национальной безопасности РА и РФ:

Основы государственной политики РА и РФ в области информационной безопасности (ИБ): Национальные интересы РА и РФ в информационной сфере и их обеспечение. Виды угроз национальной безопасности РА и РФ. Источники угроз ИБ РА и РФ

Тема 2.1. Основы государственной политики РА и РФ в области информационной безопасности (ИБ):

Основные приоритеты в области информационной безопасности РФ И РА закреплены доктринами информационной безопасности и законами, регулирующими работу средств массовой информации, законом о государственной тайне и другими нормативно-правовыми актами.

- Доктрина Информационной безопасности РФ
- Доктрина Информационной безопасности РА
- Федеральный закон от 18.03.2019 г. № 31-ФЗ О внесении изменений в статью 15–3 Федерального закона «Об информации, информационных технологиях и о защите информации»

Тема 2.2. Виды и источники угроз национальной безопасности РА и РФ.

Основные виды и источники угроз национальной безопасности РФ и РФ закреплены концепцией и доктриной национальной безопасности данных государств.

- Стратегия национальной безопасности Российской Федерации,
- Доктрина национальной безопасности Республики Армения
- Некоторые вопросы информационной безопасности республики Армения, С. Марторосян, Ереван 2007, http://www.noravank.am/upload/pdf/274_ru.pdf

Модуль 3. Информационная война

Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство. Информационное оружие, его классификация и возможности. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации.Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

Основная литература:

- «Информационные войны: история и современность», Сулейманова Ш.С., Назарова Е.А., Москва 2017г.,
- Формула информационной войны, Расторгуев С.П., Москва 1999г.,
- Философия информационной войны, Расторгуев С.П., Москва 2003г.

Тема 3.1. Информационная война, методы и средства её ведения: Информационная безопасность и информационное противоборство.

В рамках данной теми студенты изучают исторические причины возникновения информационной войны, стадии развития и современные трансформации. Исторически информационное противоборство возникло как составная часть вооруженной борьбы. Причинами его возникновения явилось стремление нападающей стороны поднять дух своих воинов и ослабить волю врага. Сегодня информационная война стала неотъемлемой частью ведения военных действий как в качестве одной из основных стадий подготовки почвы для начала военных действий, так и во время военного противостояния.

Тема 3.2. Информационное оружие, его классификация и возможности.

Информационное оружие представляет собой средства уничтожения, искажения или хищения информации; средства преодоления систем защиты; средства ограничения допуска законных пользователей; средства дезорганизации работы технических средств, компьютерных систем.

Приложение 3.

Распределение весов по видам контролей

Формы контролей	**Веса форм текущих контролей в результирующих оценках текущих контролей**			**Веса форм промежуточных контролей в оценках промежуточных контролей**			**Веса оценок промежуточных контролей и результирующих оценок текущих контролей в итоговых оценках промежуточных контролей**			**Веса итоговых оценок промежуточных контролей в результирующей оценке промежуточных контролей**	**Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля**
Вид учебной работы/контроля	**М1[4]**	**М2**	**М3**	**М1**	**М2**	**М3**	**М1**	**М2**	**М3**		
Контрольная работа											
Тест						0.5					
Курсовая работа											
Лабораторные работы											
Письменные домашние задания											
Реферат											
Эссе											
Опрос			1								
Другие формы (Указать)											
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей									0.5		
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей											
Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей											
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей											
Вес итоговой оценки 3-го промежуточного контроля в результирующей оценке промежуточных контролей										1	
Вес результирующей оценки промежуточных контролей в результирующей оценке итогового контроля											0.5
Экзамен/зачет (оценка итогового контроля)											(Экзамен) 0.5
	∑ = 1	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**

[4] Учебный Модуль

Стобалльная шкала оценки качества знаний студентов РАУ

Критерии дифференциации при оценке качества знаний студентов РАУ	**Интервалы оценок качества знаний студентов РАУ***	**Буквенные эквиваленты оценок знаний студентов РАУ**
Для квалификационных дисциплин		
ОТЛИЧНО: Выдающиеся знания с незначительными недостатками	(88≤ x ≤100)	**A**
ОЧЕНЬ ХОРОШО: Знания выше среднего стандарта, но с некоторыми недостатками	(76≤ x < 88)	**B**
ХОРОШО: Обычные надежные знания с незначительными недостатками	(64 ≤ x < 75)	**C**
УДОВЛЕТВОРИТЕЛЬНО: Неплохие знания, но со значительными недостатками	(52≤ x < 64)	**D**
ДОСТАТОЧНО: Знания соответствуют минимальным критериям	(40 ≤ x <52)	**E**
НЕУДОВЛЕТВОРИТЕЛЬНО: Неприемлемый уровень знаний и требуется некоторая дополнительная работа для получения соответствующих академических кредитов	(20 ≤ x <40)	**FX**
НЕУДОВЛЕТВОРИТЕЛЬНО: Совершенно неприемлемый уровень знаний и требуется значительная дополнительная дальнейшая работа для получения соответствующих академических кредитов.	(0≤ x <20)	**F**