ГОУ ВПО Российско-Армянский (Славянский) университет

Утверждено
Директор Института Международных отношений и
общественно-политических наук
Маргарян Е.Г.

«14» 07 2025, протокол №10

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

Наименование дисциплины: Компьютерные технологии в политических науках

Автор: Беджанян Анна Рафинадовна, старший преподаватель

Направление подготовки: 41.04.04 Политология
Наименование образовательной программы: Национальная безопасность

1. АННОТАЦИЯ

1.1. 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.

1.2. Курс «Компьютерные технологии в политических науках» тесно взаимосвязан с такими дисциплинами как «Информационная безопасность», «Основы национальной безопасности», «Медиа-планирование и медиа-анализ», «Проблемы региональной безопасности» и др..Трудоемкость в академических кредитах и часах, формы итогового контроля (экзамен/зачет); 72, зачет

1.3. Результаты освоения программы дисциплины:

Код компетенции *(в соответствии рабочим с учебным планом)*	**Наименование компетенции** *(в соответствии рабочим с учебным планом)*	**Код индикатора достижения компетенций** *(в соответствии рабочим с учебным планом)*	**Наименование индикатора достижений компетенций** *(в соответствии рабочим с учебным планом)*
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1 УК-4.2 УК-4.3	Использует информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (-ых) языках. Свободно воспринимает, анализирует и критически оценивает устную и письменную деловую информацию на русском, родном и иностранном (-ых) языке (-ах). Ведет деловую переписку, учитывая особенности стилистики официальных и неофици-альных писем,

			социокультурные различия в формате корреспонденции на государствен-ном (-ых) и иностранном (-ых) языках.
ОПК-2	Способен осуществлять поиск и применять перспективные информационно-коммуникационные технологии и программные средства для комплексной постановки и решения задач профессиональной деятельности	ОПК-2.1 ОПК-2.2 ОПК-2.3	Применяет современные технологии поиска и систематизации информации для интеграции и прогноза развития политических процессов. Использует специализированные базы данных и программные средства для оперативного поиска информации, необходимой для решения профессиональных задач. Использует специализированные базы данных и программные средства для оперативного поиска информации, необходимой для решения профессиональных задач.
ОПК-3	Способен оценивать, моделировать и прогнозировать глобальные, макрорегиональные, национально-государственные, региональные и локальные политико-культурные, социально-экономические и общественно-политические процессы на основе применения методов теоретического и эмпирического исследования и прикладного анализа	ОПК-3.1 ОПК-3.2 ОПК-3.3	Использует теоретические и эмпирические методы для оценки внутри и внешнеполитических процессов различных уровней. Проводит прикладной анализ политических процессов с использованием качественных иколичественных методов для оценки и моделирования различных политических процессов. Прогнозирует развитие ситуации в рамках решения основных внутри- и внешнеполитических проблем, в том числе затрагивающих интересы Республики Армения и Российской Федерации.
ОПК-7	Способен самостоятельно выстраивать стратегии представления результатов своей профессиональной деятельности, в том числе в публичном формате, на основе подбора соответствующих информационно-коммуникативных технологий и каналов распространения информации		Выстраивает стратегии представления результатов профессиональной деятельности с учетом их специфики и особенностей целевой аудитории. Выстраивает убедительную аргументацию для достижения целей представления результатов профессиональной

			деятельности. Подбирает информационно коммуникатив-ные технологии и каналы распространения информации общественно-политической направленности.
ПК-10	Способен осуществлять сбор и обработку информации в условиях информационной закрытости и намеренного искажения данных	ПК-10.1.	Способен получить доступ к достоверной информации. Составляет презентации и отчеты по вопросам внутренней и внешней политики.

2. УЧЕБНАЯ ПРОГРАММА

2.1. 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.

2.2. 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.

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).

В результате изучения дисциплины студент должен 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.

Трудоемкость дисциплины и виды учебной работы (в академических часах и зачетных единицах)

Виды учебной работы	Всего, в акад. часах	Распределение по семестрам					
		_1_ 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	108					
1.1. Аудиторные занятия, в т. ч.:	32	32					
1.1.1. Лекции	**16**	**16**					
1.1.2. Практические занятия, в т. ч.							
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	2	**2**					
1.1.2.5. Другое (указать)							
1.1.3. Семинары	**16**	**16**					
1.1.4. Лабораторные работы							
1.1.5. Другие виды (указать)							
1.2. Самостоятельная работа, в т. ч.:							
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**					

2.3. Содержание дисциплины

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

Разделы и темы дисциплины	Всего (ак. часов)	Лекции(ак. часов)	Семинары (ак. часов)	Лабор. (ак. часов)

1	2	3	5	6
Модуль 1. Основы информационной безопасности				
Введение				
Раздел 1. Общие проблемы информационной	**10**			
Тема 1.1. Понятие информации и информационной безопасности	**5**	**3**	**2**	
Тема 1.2. Методы нарушения конфиденциальности, целостности и доступности информации.	**5**	**3**	**2**	
Раздел 2. Проверка достоверности информации	**10**			
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. Особенности интеграционных проектов за пределами ЕС.				
Тема 2.1. Основы государственной политики РА и РФ в области информационной	**4**	**2**	**2**	
Тема 2.2. Виды и источники угроз национальной безопасности РА и РФ.	**2**	**2**		
Модуль 3. Информационная война	**10**			
Тема 3.1. Информационная война,	**5**	**3**	**2**	
Тема 3.2. Информационное оружие, его классификация и возможности.		**3**	**2**	
ИТОГО	**32**	**16**	**16**	

2.3.2. Краткое содержание разделов дисциплины в виде тематического плана

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.
Модуль.

2.3.3. Материально-техническое обеспечение дисциплины

В ходе учебного процесса необходимы комнаты с проектором и доступом в интернет.

2.4. Модульная структура дисциплины с распределением весов по формам контролей

Формы контролей	**Вес формы (форм) текущего контроля в результирующей оценке текущего контроля (по модулям)**		**Вес формы промежуточного контроля в итоговой оценке промежуточного контроля**		**Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей**		**Вес итоговой оценки промежуточного контроля в результирующей оценке промежуточных контролей (семестровой оценке)**	**Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля**
Вид учебной работы/контроля	**М1** [1]	**М2**	**М1**	**М2**	**М1**	**М2**		
Контрольная работа *(при наличии)*								
Устный опрос *(при наличии)*								
Тест *(при наличии)*		1				0,5		
Лабораторные работы *(при наличии)*								

[1] Учебный Модуль

Письменные домашние задания *(при наличии)*								
Реферат *(при наличии)*								
Эссе *(при наличии)*								
Проект *(при наличии)*								
Другие формы (при наличии)								
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей								
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 результирующей оценки промежуточных контролей в результирующей оценке итогового контроля								
Вес итогового контроля (Экзамен/зачет) в результирующей оценке итогового							0.5	0.5

контроля								
	∑ = 1	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**

Примерный перечень вопросов к экзамену по всему курсу или к каждому промежуточному и итоговому контролю для самопроверки студентов:

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.
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.

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.Какиеметоды 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.