МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ПОСТСОВЕТСКИХ И МЕЖРЕГИОНАЛЬНЫХ ИССЛЕДОВАНИЙ
Кафедра стран постсоветского зарубежья

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНОМ МЕДИА ПРОСТРАНСТВЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Институт постсоветских и межрегиональных исследований
Кафедра стран постсоветского зарубежья
Профиль «Международные отношения в Евразии: Россия и Турция в современной Евразии (внешняя политика, общество, культура)»
Уровень квалификации выпускника: бакалавр

Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

Информационная безопасность в глобальном медиа пространстве
Рабочая программа дисциплины

Составитель:
кандидат исторических наук,
доцент кафедры стран постсоветского зарубежья ИПиМИ
А.В. Гущин

УТВЕРЖДЕНО
Протокол заседания кафедры стран постсоветского зарубежья
№ 2 от 30.03.2021

ОГЛАВЛЕНИЕ

1. Пояснительная записка
1.1 Цель и задачи дисциплины *(модуля)*
1.2. Перечень планируемых результатов обучения по дисциплине (*модулю*), соотнесенных с индикаторами достижения компетенций
1.3. Место дисциплины в структуре образовательной программы
2. .Структура дисциплины *(модуля)*
3. Содержание дисциплины *(модуля)*
4. Образовательные технологии
5. Оценка планируемых результатов обучения
5.1. Система оценивания
5.2.Критерии выставления оценок
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине *(модулю)*
6. Учебно-методическое и информационное обеспечение дисциплины
6.1. Список источников и литературы
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»
7. Материально-техническое обеспечение дисциплины *(модуля)*
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов
9. Методические материалы
9.1. Планы практических (семинарских, лабораторных) занятий
9.2. Методические рекомендации по подготовке письменных работ
9.3. Иные материалы

Приложения
Приложение 1. Аннотация дисциплины
Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: ознакомить студентов с основными понятиями информационной безопасности, структурой мер в области информационной безопасности, делая особый акцент на гуманитарном измерении информационной безопасности и человеческом факторе.

Задачи дисциплины: изучить терминологию и основные понятия теории защиты информации, нормативные документы и методы защиты компьютерной информации; дать представления о тенденциях развития информационной защиты с моделями возможных угроз; рассмотреть гуманитарный аспект в защите информации и человеческий фактор в сфере угроз информационной безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине (*модулю*), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Анализирует задачу, выделяя ее базовые составляющие. Осуществляет декомпозицию задачи. УК-1.2 Находит и критически анализирует информацию, необходимую для решения поставленной задачи	Знать: методы и средства защиты компьютерной информации; терминологию и основные понятия теории защиты информации, нормативные документы. Уметь: выявлять источники, риски и формы атак на информацию, разрабатывать политику компании в соответствии со стандартами безопасности. Ориентироваться в современных аппаратно-программных решениях по защите информации.

		Владеть: основными принципами и логикой проектирования систем защиты информации и критической инфраструктуры.
ОПК-2. Способен применять информационно-коммуникационные технологии и программные средства для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры и требований информационной безопасности	ОПК-2.1. Использует информационно-коммуникационные технологии и программные средства для поиска и обработки больших объемов информации по поставленной проблематике на основе стандартов и норм, принятых в профессиональной среде, и с учетом требований информационной безопасности. ОПК-2.2. Самостоятельно каталогизирует накопленный массив информации и формировать базы данных. ОПК-2.3. Использует качественный и количественный инструментарий обработки больших массивов данных с целью выведения новой информации	Знать: меры законодательного, административного, процедурного и программно-технического уровней в контексте глобального медиапространства. Уметь: использовать нормативно-правовые знания в области информационной безопасности. Владеть: навыками анализа нормативных актов, регулирующих проблему информационной безопасности в глобальном медиапространстве.

	и получения содержательных выводов.	

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в глобальном медиа пространстве» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Введение в профессию», «Международные конфликты в XXI в.».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Экспертное сопровождение и аналитика международных отношений», «Интеграционные процессы и международные отношения в контексте политики безопасности на евразийском пространстве».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**20**
7	Семинары	**22**
7	Экзамен	**18**
Всего:		**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 48 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1.	Актуальность информационной безопасности: понятия и определения.	Основные понятия и определения в сфере информационной безопасности: защита информации, цифровые технологии, безопасность систем. Национальные интересы России в информационной сфере и их обеспечение. Международное понимание. Классификация и способы совершения компьютерных преступлений.
2.	Основные угрозы информационной безопасности в современном мире.	Основные виды и типы угроз информационной безопасности. Источники угроз. Причины уязвимости сети Интернет. Условия существования вредоносных программ. Кибератаки как фактор в современной геополитике. Хакерские атаки. Неправомерные использование и передача персональных данных пользователя. Угрозы в сфере онлайн-услуг.
3	Гуманитарный аспект и человеческий фактор в контексте проблемы информационной безопасности.	Социальная инженерия: особенности применения и меры предосторожности пользователя. «Претекстинг», «фишинг», «Троянский конь» и другие методы мошенничества в сети Интернет.
4.	Методы и средства защиты информации и обеспечения информационной безопасности.	Цифровая грамотность пользователя в контексте угроз информационной безопасности в XXI веке. Обучение граждан, направленное на повышение знаний по информационной безопасности. Регламенты по безопасности и инструкции.
5	Правовое регулирование сферы информационной безопасности.	Методы защиты конфиденциальной информации и их совершенствование: от средних веков до наших дней. Принципы правового регулирования сферы информационной безопасности в законодательстве Российской Федерации и других стран. Государственные органы РФ, контролирующие деятельность в области защиты информации. Методы защиты информации в США, Евросоюзе и других странах. Особенности «Общего регламента по защите данных» ЕС. Специалисты в сфере информационной безопасности и их подготовка как проблема XXI века для государств мира.

4. Образовательные технологии

№	Наименование раздела	Виды учебных	Образовательные технологии

п/п		занятий	
1	Актуальность информационной безопасности: понятия и определения.	Лекции Семинары Самостоятельная работа	Лекции с использованием презентации и видеоматериалов. Круглые столы по тематике семинара. Подготовка к круглым столам по тематике семинара.
2	Основные угрозы информационной безопасности в современном мире.	Лекции Семинары Самостоятельная работа	Лекции с использованием презентации и видеоматериалов. Круглые столы по тематике семинара. Подготовка к круглым столам по тематике семинара.
3	Гуманитарный аспект и человеческий фактор в контексте проблемы информационной безопасности.	Лекции Семинары Самостоятельная работа	Лекции с использованием презентации и видеоматериалов. Круглые столы по тематике семинара. Подготовка к круглым столам по тематике семинара.
4	Методы и средства защиты информации и обеспечения информационной безопасности.	Лекции Семинары Самостоятельная работа	Лекции с использованием презентации и видеоматериалов. Круглые столы по тематике семинара. Подготовка к круглым столам по тематике семинара.
5	Правовое регулирование сферы информационной безопасности.	Лекции Семинары Самостоятельная работа	Лекции с использованием презентации и видеоматериалов. Круглые столы по тематике семинара. Подготовка к круглым столам по тематике семинара.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		

- опрос *- участие в дискуссии на семинаре* *- контрольная работа (темы 1-3)* *- контрольная работа (темы 4-7)*	*5 баллов* *5 баллов* *10 баллов* *10 баллов*	*30 баллов* *10 баллов* *10 баллов* *10 баллов*
Промежуточная аттестация *(зачёт с оценкой)*		*40 баллов*
Итого за семестр *(дисциплину)* *зачёт*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворите льно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине *(модулю)*

Вопросы к зачёту

1. Методы защиты информации в XXI веке.
2. Понятие «цифровых технологий» и их применение в различных сферах жизни.
3. Национальные интересы России в информационной сфере и их обеспечение.
4. Компьютерные преступления: классификация и способы совершения.
5. Информационная безопасность. Основные источники угроз.
6. Причины уязвимости сети Интернет и условия существования вредоносных программ.
7. Вопрос информационной безопасности в современной геополитике.
8. Хакерские атаки. Причины распространения и способы противодействия.
9. Социальная инженерия: основные особенности и меры предосторожности пользователя.
10. Мошенничество в сети: основные типы и угрозы.
11. Психологические манипуляции и проблема агрессии в сети.
12. Проблема «fake news» в условиях современной геополитической напряжённости.
13. Цифровая грамотность пользователя в контексте угроз информационной безопасности в XXI веке.
14. Технические, правовые и организационные средства защиты информации.
15. Методы защиты конфиденциальной информации и их совершенствование: от средних веков до наших дней.
16. Принципы правового регулирования сферы информационной безопасности в законодательстве Российской Федерации.
17. Государственные органы РФ, контролирующие деятельность в области защиты информации.
18. Методы защиты информации в США, Евросоюзе и других странах. Особенности «Общего регламента по защите данных» ЕС.
19. Специалисты в сфере информационной безопасности и их подготовка как проблема XXI века для государств мира.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники:

1. Закон Российской Федерации от 27.12.1991 №2124-1 «О средства массовой информации» (действующая редакция от 24.11.2014)
2. О сертификации продукции и услуг/ Закон Российской Федерации

3. О федеральных органах правительственной связи и информации/ Закон Российской Федерации
4. О государственной тайне/ Закон Российской Федерации
5. Об информации, информатизации и защите информации/ Закон Российской Федерации

Основная литература:

1. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
2. Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
3. Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.
4. Медиаконвергенция, которая изменила мир? [Электронный ресурс] / Сборник статей к научно-практической конференции. Под ред. М.С. Корнева. – М., 2014. – http://www.slideshare.net/mkornev/ss-33893336
5. Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008
6. Панарин И.Н. Информационная власть и война – М: Мир безопасности, 2001
7. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие – СПб: Питер, 2008
8. СМИ в меняющейся России: Коллективная монография / Под ред. проф. Е.Л.Вартановой; науч. редактор И.Д.Фомичёва. – М.: Аспект Пресс, 2010.
9. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: учебное пособие – М: Инфра-М, 2001
10. Тенденции развития ньюзрумов - 2014. Доклад SFN №01, 2014 [Электронный ресурс] / 2-е изд. под ред. М.С. Корнева. – 116 с. – http://www.slideshare.net/mkornev/wanifra-51625489
11. Энциклопедия мировой индустрии СМИ: Учебное пособие для студентов вузов / Под ред. Е.Л.Вартановой. – М., 2013.
12. Digital-агрессия: что делать и кто виноват? [Электронный ресурс] / Сборник статей к научно-практической конференции. Под ред. М.С. Корнева. – М., 2015. -
13. Lippmann W. Public Opinion. N.Y., 1922.

Дополнительная литература:

1. Байбурин В.Б., Бровков М.Б., Пластун И.Л. Введение в защиту информации: учебное пособие – М: Инфра-М, 2004

2. Березин В.М.Массовая коммуникация: сущность, каналы, действия.- М.: Изд. РИП-холдинг, 2003.

3. Галатенко В.А. Стандарты информационной безопасности – М: ИНТУИТ.РУ, 2004

4. Горбатов В.С., Фатьянов А.А. Правовые основы защиты информации. М.:МИФИ, 2002.

5. Мельник Г. С., Ким М. Н. Методы журналистики. СПб. 2006.

6. Филин С.А. Информационная безопасность: учебное пособие – М: Альфа-Пресс, 2006

7. Ярочкин В.И. Информационная безопасность: учебное пособие – М: Международные отношения, 2000

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. РИА Новости [Электронный ресурс]. URL: http://ria.ru/
2. ИТАР-ТАСС [Электронный ресурс]. URL: http://www.itar-tass.com/
3. РосБизнесКонсалтинг// [Электронный ресурс]. URL: http://www.rbc.ru/
4. Сайт радиостанции «Эхо Москвы» [Электронный ресурс]. URL: http://echo.msk.ru/
5. Российский совет по международным делам [Электронный ресурс]. URL: https://russiancouncil.ru/

Поисковые системы

1. Яндекс [Электронный ресурс]. URL: http://www.yandex.ru/
2. Google [Электронный ресурс]. URL: http://www.google.com/
3. Yahoo [Электронный ресурс]. URL: http://www.yahoo.com
4. Спутник [Электронный ресурс]. URL: https://www.sputnik.ru/

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины «Информационная безопасность в глобальном медиа пространстве» используются: компьютерный класс с возможностью презентации в системе «Power Point», раздаточные материалы, учебные фильмы.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы семинарских занятий

Тема 1. Актуальность проблемы информационной безопасности в глобальном медиапространстве (2 часа)

Вопросы
1. Информационная безопасность как объект изучения в технических и гуманитарных науках.
2. Понятийный аппарат дисциплины. Навигация в сфере информационной безопасности.
3. Основные представления об информационной безопасности в различных государствах: экономические и культурные аспекты.

Литература:
Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Тема 2. Основные угрозы информационной безопасности в современном мире. (4 часа)

Вопросы
1. Классификация угроз в сфере информационной безопасности.
2. Неправомерные использование и передача персональных данных пользователя.
3. Кибератаки и методы предотвращения угроз в онлайн-пространстве.

Литература:
Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Тема 3. Проблема информационной безопасности и роль человеческого фактора. (2 часа)

Вопросы

1. Понятие «социальной инженерии»: основные аспекты и угрозы.
2. Психологический фактор и его применение с целью мошенничества.
3. Анонимность и агрессия в интернете.

Литература:
Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Тема 4. Проблема достоверности информации в сети Интернет (2 часа)

Вопросы
1. Информационные войны как один из инструментов глобального влияния в современном мире.
2. Проблема «fake news» как инструмента политической борьбы в XXI веке.
3. Вмешательство в выборы и влияние на их исход: реальность или вымысел?

Литература:
Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Тема 5. Методы и средства защиты информации и обеспечения информационной безопасности. (4 часа)

Вопросы

1. Технические, правовые и организационные средства защиты информации.
2. Цифровая грамотность пользователя.
3. Основные критерии безопасности информационных систем.

Литература:
Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Тема 6. Правовое регулирование сферы информационной безопасности в России (4 часа)

Вопросы

1. Принципы правового регулирования сферы информационной безопасности в законодательстве Российской Федерации.
2. Государственные органы РФ, контролирующие деятельность в области защиты информации.
3. Интернет и государство: защита граждан или цензура?

Литература:
Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Тема 7. Правовое регулирование сферы информационной безопасности в ЕС, США, Китае и других странах (4 часа)

Вопросы

1. Основные особенности регулирования сферы информационной безопасности в странах мира и их отличия от российского опыта.
2. Особенности «Общего регламента по защите данных» ЕС и оценка возможности использования схожей практики на евразийском пространстве.
3. Специалисты в сфере информационной безопасности и их подготовка как глобальный вызов XXI века.

Литература:

Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита. Спб., 2003.
Кевин Митник, Вильям Л. Саймон. Искусство обмана. М., 2004. - 131 с.
Лукина М.М. Интернет СМИ. Теория и практика. М. Аспект-Пресс.,2010, - 350с.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность в глобальном медиа пространстве» реализуется кафедрой стран постсоветского зарубежья Института постсоветских и межрегиональных исследований.

Цель дисциплины: ознакомить студентов с основными понятиями информационной безопасности, структурой мер в области информационной безопасности, делая особый акцент на гуманитарном измерении информационной безопасности и человеческом факторе.

Задачи дисциплины: изучить терминологию и основные понятия теории защиты информации, нормативные документы и методы защиты компьютерной информации; дать представления о тенденциях развития информационной защиты с моделями возможных угроз; рассмотреть гуманитарный аспект в защите информации и человеческий фактор в сфере угроз информационной безопасности.

Дисциплина направлена на формирование следующих компетенций:

УК-1
Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.
ОПК-2.
Способен применять информационно-коммуникационные технологии и программные средства для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры и требований информационной безопасности.

В результате освоения дисциплины обучающийся должен:
Знать: меры законодательного, административного, процедурного и программно-технического уровней в контексте глобального медиа пространства.

Уметь: использовать нормативно-правовые знания в области информационной безопасности.

Владеть: навыками анализа нормативных актов, регулирующих проблему информационной безопасности в глобальном медиа пространстве.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.