Федеральное государственное бюджетное образовательное учреждение высшего образования

Московский государственный институт культуры

УТВЕРЖДЕНО:
Председатель УМС
факультета Медиакоммуникаций и
аудиовизуальных искусств
Кот Ю.В.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность: 55.05.01. Режиссура кино и телевидения

Специализация: Режиссер телевизионных фильмов, телепрограмм

Квалификация (степень) выпускника: Режиссер телевизионных программ

Форма обучения: Очная

(ФОС адаптирован для лиц
с ограниченными возможностями здоровья и инвалидов)

КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций ОПК-2 и ОПК-7 в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности) *55.05.01 Режиссура кино и телевидения.*

Перечень планируемых результатов обучения по дисциплине (модулю).

Компетенция (код и наименование)	**Индикаторы компетенции**	**Результаты обучения.** ***Выпускник должен:***
ОПК-2 Способен ориентироваться в проблематике современной государственной политики Российской федерации в сфере культуры	*ОПК-2.1* Знает правовое регулирование отношений в области информационной безопасности, и может применить теоретические знания в своей профессиональной деятельности	Знать Основные теоретические и методические подходы к определению государственной культурной политики. Уметь Использовать теоретический материал для выработки понимания действия закономерностей, происходящих в современной государственной культурной политике; использовать теоретические положения для решения прикладных задач. Владеть Навыками исследования процессов современной государственной культурной политики.
ОПК-7 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1 Демонстрирует знания принципов работы современных информационных технологий ОПК-7.2 Грамотно использует принципы работы современных информационных технологий для решения профессиональных задач	Знать Основные виды современных информационных технологий и их специфические особенности Уметь Отбирать и использовать современные информационные технологии в процессе создания съемочного проекта Владеть Современными информационными технологиями

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Текущая и промежуточная аттестация по дисциплине осуществляется в соответствии со структурированным тематическим планом, а также фондом оценочных средств дисциплины, являющимся неотъемлемой частью учебно-методического комплекса.

По дисциплине предусматривается проведение:

- текущего контроля успеваемости студентов;
- промежуточной аттестации успеваемости студентов.

Текущий контроль – это непрерывно осуществляемое наблюдение за уровнем усвоения знаний и формирования умений и навыков в течение семестра.

Промежуточная аттестация – это вид контроля, предусмотренный рабочим учебным планом направления подготовки, осуществляется в ходе зачета.

Система оценивания

Форма контроля	**Оценка**
Текущий контроль: *- опрос* *- участие в дискуссии на практическом занятии* *- тестовые задания*	*зачтено/не зачтено* *Зачтено (не менее 50% ответов даны правильно) / не зачтено (менее 50 % ответов даны правильно)*
Промежуточная аттестация Экзамен	*Отлично/хорошо/удовлетворительно/неудовлетворительно*

Критерии оценки результатов по дисциплине

Оценка по дисциплине	**Критерии оценки результатов обучения по дисциплине**
«Отлично»/ зачтено	Выставляется обучающемуся, если компетенция, закрепленная за дисциплиной, сформирована (по индикаторам/ результатам обучения в формате «знать-уметь-владеть») в полном объеме на уровне «высокий». При этом студент глубоко и всесторонне усвоил проблему; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет терминологией по дисциплине.
«Хорошо»/ зачтено	Выставляется обучающемуся, если компетенция, закрепленная за дисциплиной, сформирована (по индикаторам/ результатам обучения в формате «знать-уметь-владеть») на уровне «хороший». При этом студент твердо усвоил тему, грамотно и по существу излагает ее, опираясь на знания основной литературы; - не допускает существенных неточностей;

	- увязывает усвоенные знания с практической деятельностью; - аргументирует научные положения; - делает выводы и обобщения; - владеет терминологией по дисциплине
«Удовлетворительно»/ зачтено	Выставляется обучающемуся, если компетенция, закрепленная за дисциплиной, сформирована (по индикаторам/ результатам обучения в формате знать-уметь-владеть) на уровне «удовлетворительный». При этом тема раскрыта недостаточно четко и полно, то есть студент освоил проблему, по существу излагает ее, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении психологических знаний; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет терминологией по дисциплине.
«Неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если компетенция, закрепленная за дисциплиной, не сформирована (по индикаторам/ результатам обучения в формате «знать-уметь-владеть»), то есть результаты обучения ниже удовлетворительного уровня. Студент не усвоил значительной части проблемы; - допускает существенные ошибки и неточности при рассмотрении ее; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений; - не владеет терминологией по дисциплине

Примеры практических заданий:

1. Сделать видеосюжет об информационных войнах
2. Сделать видеосюжет на тему актуальности семи правил М.В. Ломоносова для журналистов
3. Сделать видеосюжет на тему «Быть русским»
4. Сделать видеосюжет на тему «Русская голгофа»

Примерные вопросы к зачету:

1. Назовите основные источники получения информации
2. Назовите 7 правил М.В. Ломоносова для журналистов
3. Информационные войны. Инструментарий их ведения, цели, которые они преследуют
4. Законы РФ о СМИ
5. Основные критерии определения фейка в информационном пространстве
6. Доктрина информационной безопасности России

7. Защита ПК от несанкционированного доступа
8. Информационные технологии
9. Основные задачи в сфере обеспечения информационной безопасности.

Примерные вопросы к экзамену:

1. Назовите методы определения недостоверных данных в информационном пространстве
2. Основные понятия информационной безопасности
3. Государственное регулирование информационной безопасности
4. Назовите технологии манипуляции общественным сознанием, основные информационные технологии
5. Основные критерии определения фейка в информационном пространстве
6. Информационные технологии.
7. Система защиты информации и ее структуры.
8. Персональные данные и их защита.
9. Информационные угрозы, их виды и причины возникновения.
10. Информационные угрозы для государства.
11. Информационные угрозы для компании.
12. Информационные угрозы для личности (физического лица).
13. Действия и события, нарушающие информационную безопасность.
14. Способы воздействия информационных угроз на объекты.
15. Деятельность международных организаций в сфере информационной безопасности.
16. Федеральные законы в сфере информатизации и информационной безопасности.
17. Политика безопасности и ее принципы.
18. Методы и средства защиты информации.
19. Защита информации в Интернете.
20. Принципы противодействия мобильным мошенникам, пошагово.
21. Понятие информационной войны. Особенности информационной войны.
22. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
23. Сфера применения информационного оружия.
24. Основные задачи в сфере обеспечения информационной безопасности.
25. Защита ПК от несанкционированного доступа.
26. Дипфейк.
27. Принципы работы ЦИПСО в информационной среде.
28. Технология цветных революций. Основные механизмы противодействия.