МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра журналистики и массовых коммуникаций

Авторы-составители: **Печищев Иван Михайлович**

Рабочая программа дисциплины

МЕДИЙНАЯ И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ И БЕЗОПАСНОСТЬ

Код УМК 93623

Утверждено
Протокол №9
от «17» июня 2019 г.

Пермь, 2019

1. Наименование дисциплины

Медийная и информационная грамотность и безопасность

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление: **46.03.01** История

направленность Программа широкого профиля

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Медийная и информационная грамотность и безопасность** у обучающегося должны быть сформированы следующие компетенции:

46.03.01 История (направленность : Программа широкого профиля)

ОПК.2 Способен применять информационно-коммуникационные технологии в профессиональной деятельности

Индикаторы

ОПК.2.1 Ориентируется в информационно-коммуникационных технологиях и программных средствах для поиска и обработки информации с учетом требований информационной безопасности

УК.12 Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

4. Объем и содержание дисциплины

Направления подготовки	46.03.01 История (направленность: Программа широкого профиля)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	7
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	14
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (7 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Медийная и информационная грамотность и безопасность

Курс посвящен знакомству с информационной средой, получению навыков фильтрации информации, критического мышления и защиты своих цифровых данных. Курс призван научить основам эффективной и безопасной жизни в онлайн-среде. Он дает представление о разнообразных угрозах интернета. Большое внимание уделяется необходимым мерам безопасности

Угрозы интернета и социальных сетей

Данный раздел посвящен разнообразным угрозам интернета и социальных сетей. Они не только рассматриваются «изнутри», студенты в то же время получают информацию, как защититься от этих угроз.

Введение: что и как защищать

Обзор основных угроз интернета и социальных сетей: что и кто угрожает пользователю, чем рискует каждый пользователь интернета, какие данные наиболее уязвимы. Анализ различных сценариев угроз пользователю.

Деловая игра «Медиапасьянс»

В деловой игре студенты познакомятся с основными угрозами интернета и социальных сетей и главными источниками информации. В игровой форме студенты определят сценарии возможных угроз на различных платформах, сделают вывод о необходимости защиты, определят наиболее уязвимые данные.

Как защититься от угроз интернета и социальных сетей: мошенничество, рекламодатели

Обзор наиболее распространённых сценариев взаимодействия с мошенниками и рекламодателями. Анализ целей взаимодействия, их возможностей, угроз. Отдельно будут рассмотрены способы защиты от мошенников и рекламодателей в интернете

Как защититься от угроз интернета и социальных сетей: противоправная деятельность

Обзор наиболее распространенных сценариев вовлечения в противоправную деятельность и угроз, связанных со взаимодействием с противоправным контентом. Какие методы используют преступники в интернете, сценарии коммуникации, анализ их целей. Основные приемы защиты от преступников в интернете. Анализ правоприменительной практики по поводу взаимодействия с противоправным контентом, угрозы и риски, сценарии поведения пользователей.

Как защититься от угроз интернета и социальных сетей: кибербуллинг, доксинг

Обзор наиболее распространенных сценариев кибербуллинга и доксинга в сети. Анализ целей коммуникации, возможностей преступников, угроз. Основные приемы защиты и профилактики.

Как защитить свой аккаунт

Способы защиты аккаунта в интернете. Методы создания надежного пароля, двухфакторная аутентификация, подтверждение входа. Вход в аккаунт на чужом компьютере. Использование специальных сервисов и приложений.

Приватность в интернете и социальных сетях

Зачем нужна приватность и как её сохранить. Настройки приватности в социальных сетях. Программное обеспечение и приложения для сохранения приватности в интернете. Основные методы безопасной работы в интернете. Использование публичного WiFi, безопасные протоколы HTTPS, проверка подозрительных ссылок, приватный режим браузера, плагины для приватности, использование VPN. Безопасная работа в интернете.

Базовая защита устройств

Основные методы защиты компьютера, смартфона и других устройств. Лицензионное и свободное программное обеспечение, антивирус, автозапуск устройств, подозрительное программное обеспечение для компьютера и смартфона, пароль на вход в устройство, опасность веб-камеры

Медиаграмотность и новостная грамотность

Данный раздел посвящен изучению медиаграмотности и новостной грамотности. Они не только рассматриваются «изнутри», студенты в то же время получают основные навыки работы с информацией

Фейки и дезинформация

Почему важно быть медиаграмотным. Что такое фейк, зачем он создаётся и как распространяется. Обзор кейсов. Виды дезинформации, её назначение и применение. Опасности дезинформации для современного общества

Фактчекинг: инструменты и методы

Фактчекинг как важный инструмент современных специалистов в сфере медиа. Способы проверки информации: поиск фактов, обратный поиск фотографий, проверка источников (аккаунты, сайты). Онлайн-сервисы проверки информации, алгоритмы контента.

Информационная гигиена

Цифровая гигиена – почему это важно. Как устроена лента социальной сети. Как настроить ленту по своим интересам. Как настроить сбор и хранение информации

Деловая игра «Круг доверия»

В деловой игре студенты определят источники информации, которыми они пользуются, которым доверяют или не доверяют. Кроме этого студенты оценят доверие к различным форматам контента. Таким образом будет сформирована карта медиапотребления каждого студента, определён “пузырь фильтров" каждого студента. В ходе игры будет рассмотрено воздействие разных информационных источников на отдельных студентов и вымышленных персонажей. Будет обсужден вопрос воздействия информационной среды на отдельного индивидуума

Когнитивные искажения аудитории

Какими бывают когнитивные искажения. Классификация когнитивных искажений. Их роль в медиапотребления и жизни каждого пользователя интернета. Кейсы проявления когнитивных искажений. Движение “плоская Земля" как яркий пример когнитивного искажения аудитории.

Создание проекта по медиаграмотности

Создание группового цифрового проекта по медиаграмотности для заданной аудитории. Создание советов по медийной или новостной грамотности, либо по информационной безопасности в формате инфографике, видео, анимации и т.п.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Мультимедийная журналистика [Электронный ресурс] : учебник для вузов/ под общ. ред. А. Г. Качкаевой, С А. Шомовой; Нац. исслед. ун-т «Высшая школа экономики». — 2-е изд. (эл.). — Электрон, текстовые дан. (1 файл pdf: 418 с). — М.: Изд. дом Высшей школы экономики, 2018. — (Учебники Высшей школы экономики). — Систем, требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10". - ISBN 978-5-7598-1663-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1018960 (дата обращения: 01.09.2020). – Режим доступа: по подписке. https://elis.psu.ru/node/619650

2. Как новые медиа изменили журналистику. 2012—2016 / А. Амзин, А. Галустян, В. Гатов [и др.] ; под редакцией С. Балмаева, М. Лукиа. — Москва, Екатеринбург : Кабинетный ученый, Гуманитарный университет, 2016. — 304 c. — ISBN 978-5-7525-3084-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/75003.html

Дополнительная:

1. Компьютерная безопасность для школьников и родителей:учебное пособие/Д. А. Алдарова [и др.].-Пермь:ПГНИУ,2019, ISBN 978-5-7944-3251-0.-80.-Библиогр. в конце ст. https://elis.psu.ru/node/566518

2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 c. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/77320.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

classroom.google.com Google Classroom
www.socrative.com Socrative
www.tilda.cc Tilda
https://howsecureismypassword.net/ How Secure Is My Password?

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Медийная и информационная грамотность и безопасность** предполагает использование следующего программного обеспечения и информационных справочных систем:
1) презентационные материалы (слайды по темам лекционных и практических занятий);
2) доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
3) доступ в электронную информационно-образовательную среду университета;
4) интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта);

Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:
1) офисный пакет приложений (текстовый процессор, программа для подготовки электронных презентаций);
2) программа демонстрации видеоматериалов (проигрыватель)
Дисциплина не предусматривает использование специального программного обеспечения.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий, занятий семинарского типа, групповой работы и текущего контроля предусматривается аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для самостоятельной работы предусматривается аудитория для самостоятельной работы, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченная доступом в электронную информационно-образовательную среду университета. Помещения Научной библиотеки ПГНИУ.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:
1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с

доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Медийная и информационная грамотность и безопасность

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.2

Способен применять информационно-коммуникационные технологии в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.2.1 Ориентируется в информационно-коммуникационных технологиях и программных средствах для поиска и обработки информации с учетом требований информационной безопасности	Знает информационно-коммуникационные технологии и программные средства для поиска и обработки информации, умеет использовать информационно-коммуникационные технологии и программные средства, владеет технологиями с учетом требований информационной безопасности	**Неудовлетворител** Не знает информационно-коммуникационные технологии и программные средства для поиска и обработки информации, не умеет использовать информационно-коммуникационные технологии и программные средства, не владеет технологиями с учетом требований информационной безопасности **Удовлетворительн** Частично знает информационно-коммуникационные технологии и программные средства для поиска и обработки информации, частично умеет использовать информационно-коммуникационные технологии и программные средства, частично владеет технологиями с учетом требований информационной безопасности **Хорошо** В основном знает информационно-коммуникационные технологии и программные средства для поиска и обработки информации, в основном умеет использовать информационно-коммуникационные технологии и программные средства, в основном владеет технологиями с учетом требований информационной безопасности **Отлично** Знает информационно-коммуникационные технологии и программные средства для поиска и обработки информации, умеет использовать информационно-коммуникационные технологии и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично программные средства, владеет технологиями с учетом требований информационной безопасности

УК.12

Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.12 Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Знает сущность и значение информации в развитии современного общества, умеет соблюдать основные требования информационной безопасности, владеет навыком защиты государственной тайны.	**Неудовлетворител** Не знает сущность и значение информации в развитии современного общества, не умеет соблюдать основные требования информационной безопасности, не владеет навыком защиты государственной тайны. **Удовлетворительн** Частично знает сущность и значение информации в развитии современного общества, частично умеет соблюдать основные требования информационной безопасности, частично владеет навыком защиты государственной тайны. **Хорошо** В основном знает сущность и значение информации в развитии современного общества, в основном умеет соблюдать основные требования информационной безопасности, в основном владеет навыком защиты государственной тайны. **Отлично** Знает сущность и значение информации в развитии современного общества, умеет соблюдать основные требования информационной безопасности, владеет навыком защиты государственной тайны.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 45 до 60
«неудовлетворительно» / «незачтено» менее 45 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Введение: что и как защищать **Входное тестирование**	Знания о современной медиасфере, рисках и угрозах интернета
ОПК.2.1 Ориентируется в информационно-коммуникационных технологиях и программных средствах для поиска и обработки информации с учетом требований информационной безопасности **УК.12** Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Как защитить свой аккаунт **Защищаемое контрольное мероприятие**	Знает виды угроз в интернете, цели цифровых преступников и их методы, способы защиты аккаунтов. Умеет видеть опасности в интернете, выстраивать защиту от них. Владеет технологиями защиты аккаунта
ОПК.2.1 Ориентируется в информационно-коммуникационных технологиях и программных средствах для поиска и обработки информации с учетом требований информационной безопасности	Фактчекинг: инструменты и методы **Защищаемое контрольное мероприятие**	Знает о видах дезинформации, умеет выбрать инструмент для проверки контентом, владеет технологиями фактчекинга

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.2.1 Ориентируется в информационно-коммуникационных технологиях и программных средствах для поиска и обработки информации с учетом требований информационной безопасности **УК.12** Способен понимать сущность и значение информации в развитии современного общества, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	Создание проекта по медиаграмотности **Итоговое контрольное мероприятие**	Знает основы медиаграмотности, умеет объяснить риски и угрозы в медиасфере, владеет технологиями создания контента на тему медиаграмотности

Спецификация мероприятий текущего контроля

Введение: что и как защищать

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Вопросы 1—6 теста (по 1 баллу)	6
Вопрос 7 теста	4

Как защитить свой аккаунт

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **14**

Показатели оценивания	Баллы
Проведен анализ уязвимости существующих аккаунтов	10
Настройка подтверждения входа в аккаунты	10
Проведен анализ существующих паролей, выбран надежный пароль одним из изученных методов	10
За каждую допущенную ошибку снимется один балл.	-1

Фактчекинг: инструменты и методы

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **14**

Показатели оценивания	Баллы
Разоблачение дезинформации с помощью онлайн-инструментов	10
Проверка фактов в верифицированном источнике	10
Определение источника данных	5
Выбор верного инструмента для проверки информации	5
За каждую допущенную ошибку снимется один балл.	-1

Создание проекта по медиаграмотности

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Выбрана актуальная тема для медиапроекта о медиаграмотности	10
Советы по медиаграмотности точны и понятны	10
Выбран подходящий формат для медиапроекта	10
Презентация медиапроекта отражает наиболее важные стороны проекта	10
За каждую допущенную ошибку снимется один балл.	-1