

МИНОБРНАУКИ РОССИИ

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

Кафедра журналистики и массовых коммуникаций

Авторы-составители: **Печищев Иван Михайлович
Черепанова Лариса Львовна**

Кафедра СГПИ филиал ПГНИУ - математических и естественнонаучных дисциплин

Авторы - составители: (СГПИ) **Рихтер Татьяна Васильевна**

Рабочая программа дисциплины
**МЕДИЙНАЯ И ИНФОРМАЦИОННАЯ ГРАМОТНОСТЬ И
БЕЗОПАСНОСТЬ**
Код УМК 93623

Утверждено
Протокол №9
от «23» мая 2023 г.

Пермь, 2023

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 подготовки: **37.03.01** Психология
направленность Психология

3. Планируемые результаты обучения по дисциплине

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

37.03.01 Психология (направленность : Психология)

УК.13 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма и противодействовать им в профессиональной деятельности

Индикаторы

УК.13.3 Осуществляет взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности

ОПК.2 Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Индикаторы

ОПК.2.1 Демонстрирует базовые знания в области информационно-коммуникационных технологий

ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности

4. Объем и содержание дисциплины

Направление подготовки	37.03.01 Психология (направленность: Психология)
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

Медиаграмотность и новостная грамотность

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.

Медиаграмотность. Предмет изучения. Роль в современном мире

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.

Проблема идентификации сообщения в медиaprостранстве

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

Дезинформация. Методы проверки информации

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

Оценка источников информации

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

Постправда. Медиаосознанность. Критическое мышление

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

Медиапроекты по фактчекингу: мировой и российский опыт

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

Аудитория современных медиа: её особенности и характеристики

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.

Работа с кейсом по исправлению ошибок в новостных материалах СМИ

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.

Работа с кейсом по исправлению ошибок в материалах PR, соцсетях

Аудитория как участник информационно-коммуникационных процессов

Угрозы интернета и социальных сетей

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

Угрозы интернета и социальных сетей: информационная безопасность

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

Приватность в интернете и социальных сетях

В деловой игре студенты определяют 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

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 инфографики, 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. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544290>
2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. <http://www.iprbookshop.ru/97562>
3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544029>

Дополнительная:

1. Мурюкина, Е. В. Медиаобразовательные технологии в реализации образовательных программ : учебное пособие / Е. В. Мурюкина ; под редакцией Т. Н. Владимировой. — Москва : Московский педагогический государственный университет, 2021. — 144 с. — ISBN 978-5-4263-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. <https://www.iprbookshop.ru/122450>
2. 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.
3. 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 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/77320.html>
4. Медиаинформационная грамотность и современное информационное пространство : учебное пособие / Т. К. Смыковская, Н. В. Лобанова, Ю. А. Машевская [и др.]. — Волгоград : Волгоградский государственный социально-педагогический университет, «Перемена», 2020. — 184 с. — ISBN 978-5-9935-0421-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/103039.html>
5. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978-5-4497-2418-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/133957.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:

- презентационные материалы;
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.

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

Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:

ПО: ОС Microsoft Windows (предустановленная версия - OEM или версия согласно лицензионным соглашениям); пакет офисных приложений Microsoft Office (версия согласно лицензионным соглашениям); Kaspersky Endpoint Security for Business, Справочно-правовая система «КонсультантПлюс».

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.

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

Учебная аудитория для проведения занятий лекционного типа:

Основное оборудование: специализированная мебель, меловая доска, ноутбук, проектор, экран.

Для самостоятельной работы: аудитория для самостоятельной работы, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченной доступом в электронную информационно-образовательную среду университета.

Помещение научной библиотеки СГПИ филиал ПГНИУ для обеспечения самостоятельной работы обучающихся:

Помещение Научной библиотеки СГПИ филиал ПГНИУ, оснащенное компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ПГНИУ.

Основное оборудование: специализированная мебель, меловая доска, проектор, экран, ноутбуки, телевизор.

ПО: ОС Microsoft Windows (предустановленная версия - OEM или версия согласно лицензионным соглашениям); пакет офисных приложений Microsoft Office (версия согласно лицензионным соглашениям); Kaspersky Endpoint Security for Business. Справочно-правовая система «Консультант Плюс. Яндекс.Браузер (свободно распространяемое ПО) и/или Google Chrome (свободно распространяемое ПО); ОС «Альт Образование».

**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 понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.2.2 Оrientируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности 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-

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично коммуникационные технологии и программные средства, владеет технологиями с учетом требований информационной безопасности
ОПК.2.1 Демонстрирует базовые знания в области информационно-коммуникационных технологий	Знает специфику современной информационной среды, умеет ориентироваться в многообразии информационно-коммуникационных технологий, владеет методами работы с информационной средой и информационно-коммуникационными технологиями.	Неудовлетворител Не знает специфику современной информационной среды, не умеет ориентироваться в многообразии информационно-коммуникационных технологий, не владеет методами работы с информационной средой и информационно-коммуникационными технологиями. Удовлетворительн В целом знает специфику современной информационной среды, умеет ориентироваться в многообразии информационно-коммуникационных технологий, но допускает ошибки, владеет отдельными методами работы с информационной средой и информационно-коммуникационными технологиями. Хорошо В целом знает специфику современной информационной среды, умеет ориентироваться в многообразии информационно-коммуникационных технологий, но допускает отдельные ошибки, владеет основными методами работы с информационной средой и информационно-коммуникационными технологиями. Отлично Знает специфику современной информационной среды, умеет ориентироваться в многообразии информационно-коммуникационных технологий, владеет методами работы с информационной средой и информационно-коммуникационными технологиями.

УК.13

Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма и противодействовать им в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.13.3 Осуществляет взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности	Знание специфики проявления экстремизма и терроризма, умение распознавать проявление экстремизма и терроризма в медийной среде, владение навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности.	Неудовлетворител Не знает специфику проявления экстремизма и терроризма, не умеет распознавать проявление экстремизма и терроризма в медийной среде, не владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности Удовлетворительн Знает специфику проявления экстремизма и терроризма, не во всех случаях умеет распознавать проявление экстремизма и терроризма в медийной среде, слабо владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности Хорошо Знает специфику проявления экстремизма и терроризма, умеет распознавать проявление экстремизма и терроризма в медийной среде, владеет не всеми навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности Отлично Знает специфику проявления экстремизма и терроризма, умеет распознавать проявление экстремизма и терроризма в медийной среде, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности

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	Медиаграмотность. Предмет изучения. Роль в современном мире Входное тестирование	Знания о современной медиасфере, рисках и угрозах интернета
ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно- коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности ОПК.2.1 Демонстрирует базовые знания в области информационно- коммуникационных технологий	Оценка источников информации 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.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно- коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Работа с кейсом по исправлению ошибок в новостных материалах СМИ 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 Демонстрирует базовые знания в области информационно-коммуникационных технологий ОПК.2.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности УК.13.3 Осуществляет взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности	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

Медиаграмотность. Предмет изучения. Роль в современном мире

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

Оценка источников информации

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

Работа с кейсом по исправлению ошибок в новостных материалах СМИ

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

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставяемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **14**

Показатели оценивания	Баллы
Проверка фактов в верифицированном источнике	10
Разоблачение дезинформации с помощью онлайн-инструментов	10
Выбор верного инструмента для проверки информации	5
Определение источника данных	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, выставяемый 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