МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
журналистики и литературы

Гордеев Ю.А.
18.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О3 Информационная безопасность в медиапроизводстве

1. Код и наименование направления подготовки: 42.04.02 Журналистика

2. Программа подготовки: Бизнес-журналистика и корпоративные медиакоммуникации

3. Квалификация выпускника: магистр

4. Форма обучения: заочная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра журналистики и литературы

6. Составители программы: Жолудь Роман Владимирович, кандидат филологических наук, доцент

7. Рекомендована: НМС факультета журналистики, протокол № 8 от 18.05.2023 г.

8. Учебный год: 2024-2025 **Семестр(ы):** 3

9. **Цели и задачи учебной дисциплины**

Цель учебной дисциплины: формирование знаний и умений в сфере обеспечения информационной безопасности в медиапроизводстве.

Задачи учебной дисциплины:

Задачи лекционных занятий:

– изучение основных угроз информационной безопасности в медиапроизводстве, их носителей и методов защиты от них;

– формирование системных представлений об аудите и политике информационной безопасности в медиапроизводстве.

Задачи практических занятий:

– освоение методик проведения аудита информационной безопасности и создания политики информационной безопасности в медиапроизводстве;

– изучение программных продуктов для обеспечения информационной безопасности в медиапроизводстве.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина относится к обязательной части блока Б1 учебного плана подготовки магистров по направлению 42.04.02 Журналистика.

Требования к входным знаниям, умениям и навыкам включают в себя:

– базовые представления о функционировании персональных компьютеров и интернета;

– навыки работы с персональными комрьютерами и смартфонами на уровне пользователя;

– навыки работы с офисными приложениями.

Дисциплины, для которых данная дисциплина является предшествующей: –

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-6	Способен отбирать и внедрять в процесс медиапроизводства современные технические средства и информационно-коммуникационные технологии	ОПК-6.1 ОПК-6.2	Отслеживает глобальные тенденции модернизации технического оборудования, программного обеспечения и расходных материалов, необходимых для осуществления профессиональной деятельности. Отбирает и внедряет в профессиональную деятельность современные технологии рекламы и связей с общественностью, цифровые инструменты, технические средства и программное обеспечение	Знать: основные источники угроз для информационной безопасности офиса и сотрудников, основные уязвимые информационные объекты и характер их уязвимости, основные средства защиты и обеспечения безопасной работы с информацией, принциры создания политики безопасности. Уметь: оценивать угрозы для информационной безопасности, предпринимать действия для минимизации угроз для информации, создавать политику информационной безопасности офиса. Владеть: приложениями и сервисами, обеспечивающими безопасность информации, хранящейся на электронных носителях, в веб-ресурсах, передающейся по различным каналам связи
ПК-3	Способен про-	ПК)-3.2	Определяет поле иссле-	Уметь: определять границы охвата по-

	водить научное исследование в сфере журналистики и медиа на основе самостоятельно разработанной или адаптированной методологии и методики.		дования, разрабатывает или адаптирует методологию.	литики информационной безопасности в зависимости от условий функционирования СМИ
		ПК-3.3	Собирает и анализирует информацию, применяя избранную методику, и формулирует полученные результаты	Владеть: методами аудита и сбора информации для составления политики информационной безопасности редакции СМИ
		ПК-3.1	Проводит многофакторный анализ перспектив запуска проекта в медиасфере	Уметь: оценивать эффективность и анализировать результаты внедрения политики информационной безопасности редакции СМИ

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			3
Аудиторные занятия		12	12
в том числе:	лекции	12	12
	практические	–	–
Самостоятельная работа		87	87
Форма промежуточной аттестации – экзамен		9	9
Итого:		108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Общие принципы информационной безопасности	Понятие информационной безопасности. Уязвимости, их причины. Базы данных и архивы, чувствительная и конфиденциальная информация, финансовая информация. Веб-сайт и домен, аккаунты в социальных медиа. Электронная почта. Мобильные телефрны. Основные угрозы для информационной безопасности. Техногенные и природные угрозы. Фишинг. Ви-	–

		русы. Перехват информации. Атаки на сайт.	
1.2	Методы укрепления информационной безопасности	Общие подходы к укреплению информационной безопасности. Персональная и корпоративная информационная безопасность. Создание политики безопасности. Резервное копирование информации. Политика безопасных паролей. Средства шифрования. Антивирусы и firewall. Защита хостинга. Защита мобильных телефонов. Безопасный серфинг. Сервисы VPN.	–
1.3	Технологии и методики безопасной коммуникации	Внутрикорпоративная коммуникация. Безопасные чаты и облачные ресурсы для хранения и обмена информацией. Организация защищенных аудио- и видеоконференций. Организация совместной удаленной работы над проектом.	–
2. Практические занятия			
2.1	Программное обеспечение для защиты информации	Менеджеры паролей. Программы для шифрования информации, особенности их работы. Синхронизация данных. Программы и сервисы для резервного копирования.	–
2.2	Создание безопасных паролей	Способы взлома паролей. Методы противостояния взлому паролей. Требования к безопасному паролю.	–
2.3	**Проведение онлайн-конференций и организация совместной удаленной работы**	Приложения и сервисы для видеоконференций, их сравнительный анализ. Приложение Zoom, его функции и возможности. Приложения и сервисы для удаленной совместной работы, их сравнительная характеристика. Сервис Trello, его функции и возможности.	–

13.2 Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Практ. занятия	Самостоятельная работа	Всего
1	Общие принципы информационной безопасности	4		40	44
2	Методы укрепления информационной безопасности	4		30	44
3	Технологии и методики безопасной коммуникации	4		7	11
	Итого:	12		87	99

14. Методические указания для обучающихся по освоению дисциплины

Часть учебного материала изучается и на лекциях, и на практических занятиях, часть – только на лекциях или только на практических занятиях. Практические занятия представляют собой семинары по изучаемому материалу: на каждом занятии студенты получают домашнее задание и отчитываются о его выполнении на следующем занятии. Предусмотрена текущая аттестация в форме контрольных работ (тестов) по материалу, пройденному в течение семестра. Самостоятельная работа студента предполагает:

– изучение презентационного материала лекций;
– изучение рекомендованной основной и дополнительной литературы;
– подготовку к практическим занятиям;
– подготовку к текущей аттестации (контрольным работам);
- подготовка и выполнение итогового практического задания;
– подготовку к промежуточной аттестации.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Калмыков А. А., Коханова Л. А. Интернет-журналистика: учебное пособие. - Москва: Юнити, 2015. - URL: https://biblioclub.ru/index.php?page=book_red&id=436712.
2	Олешко Е. В. Конвергентная журналистика : профессиональная культура субъектов информационной деятельности: учебное пособие. - Москва: ФЛИНТА, 2017. - URL: https://biblioclub.ru/index.php?page=book_red&id=482239.

б) дополнительная литература:

№ п/п	Источник
3	Артемов А. В. Информационная безопасность. Курс лекций. - М., 2014.
4	Калмыков, А.А. Интерактивная гипертекстовая журналистика в системе отечественных СМИ / А.А. Калмыков. – Москва ; Берлин : Директ-Медиа, 2016. – 97 с. – URL: https://biblioclub.ru/index.php?page=book&id=428741.
5	Наумов В. Б. Право и Интернет: очерки теории и практики / В.Б. Наумов; Науч. ред. В. Б. Исаков; Рос. фонд прав. реформ .— М. : Университет, 2002 .— 430 с.
6	Перфильев Ю. Ю. Российское интернет-пространство: развитие и структура / Ю.Ю. Перфильев .— М. : Гардарики, 2003. — 220 с.
7	Рассолов И. М. Интернет-право : учебное пособие для студ. вузов / И. М. Рассолов ; Моск. ун-т МВД России; Фонд содействия правоохран. органам "Закон и право" .— М. : Закон и право : ЮНИТИ-ДАНА, 2004 .— 143 с.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
8	Электронный каталог Научной библиотеки Воронежского государственного университета. — (http://lib.vsu.ru)
9ё	Электронный университет. URL: https://edu.vsu.ru
10	Университетская библиотека онлайн. Электронная библиотечная система. URL: https://www.biblioclub.ru.

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
2	Security in a Box. Инструменты и рекомендации по цифровой безопасности. – URL: https://securityinabox.org/ru/

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины проводятся занятия лекционного типа (лекции с демонстрацией презентационного материала), занятия семинарского типа (опрос, дискуссия), текущая аттестация (тестирование).

При реализации дисциплины используются элементы электронного обучения (ЭО) и дистанционные образовательные технологии (ДОТ) – смешанное обучение.

Электронный курс на платформе «Электронный университет»: https://edu.vsu.ru/course/view.php?id=9962.

18. Материально-техническое обеспечение дисциплины:

Аудитории для проведения занятий лекционного типа. Типовое оснащение, оборудование: мультимедиапроектор View Sonic; ПК (i5/4Gb/HDD 1Tb); экран настенный с электроприводом CS 244*244; акустическая система BEHRINGER B115D, микшер UB 1204 FX, микрофон B-1. Программное обеспечение: WinPro 8 RUS Upgrd OLP NL Acdmc; OfficeSTD 2013 RUS OLP NL Acdmc; неисключительные права на ПО Dr. Web Enterprise Security Suite, комплексная защита Dr. Web Desktop Security Suite + Центр управления на 12 месяцев, 1400 ПК (Продление).

Аудитории для проведения занятий семинарского типа, текущего контроля и промежуточной аттестации. Типовое оснащение, оборудование: мультимедиапроектор BenQ; экран настенный CS 244*244; переносной ноутбук 15*Packard Bell. Программное обеспечение: WinPro 8 RUS Upgrd OLP NL Acdmc; OfficeSTD 2013 RUS OLP NL Acdmc; неисключительные права на ПО Dr. Web Enterprise Security Suite, комплексная защита Dr. Web Desktop Security Suite + Центр управления на 12 месяцев, 1400 ПК (Продление).

Аудитории для самостоятельной работы студентов. Используются компьютерные классы: ауд. 115 (Воронеж, ул. Хользунова, 40-а). Типовое оснащение, оборудование: мультимедиапроектор BenQ MX511; экран настенный CS 244*244; интерактивная доска Promethean; ПК (i5/4Gb/HDD 1Tb) (11 шт.); ауд. 126 (Воронеж,

ул. Хользунова, 40-а). Типовое оснащение, оборудование: мультимедиапроектор BenQ MX511; ПК (Razer 5/4Gb/1Tb) (10 шт.); экран настенный CS 244*244; интерактивная доска Promethean. Программное обеспечение: WinPro 8 RUS Upgrd OLP NL Acdmc; OfficeSTD 2013 RUS OLP NL Acdmc; неисключительные права на ПО Dr. Web Enterprise Security Suite, комплексная защита Dr. Web Desktop Security Suite + Центр управления на 12 месяцев, 1400 ПК (Продление). Права на программы для ЭВМ Creative Cloud for teams All Apps ALL Multiple; СПС «ГАРАНТ-Образование». Свободный доступ в интернет.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Общие принципы информационной безопасности	ОПК-6	ОПК-6.1, ОПК-6.2	Практическое задание №1
2	Методы укрепления информационной безопасности	ОПК-6, ПК-3	ОПК-6.1, ОПК-6.2, ПК-3.1, ПК-3.2	Контрольная работа
3	Технологии и методики безопасной коммуникации	ОПК-6, ПК-3	ОПК-6.1, ОПК-6.2, ПК-3.3	Опрос
Промежуточная аттестация форма контроля – экзамен				Устный ответ

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:
Опрос.
Практические задания.
Контрольная работа.

Перечень заданий

Практическое задание. Описание угроз для информационной безопасности учебной лаборатории

Описание технологии проведения

Обучающим дается задание составить список угроз и вариантов их нейтрализации для учебной лаборатории (компьютерного класса). Задание выполняется письменно в течение 2 часов.

Требования к выполнению заданий, шкалы и критерии оценивания

Оценивание проводится по двухбалльной системе. Критерии оценивания включают в себя:
– наличие достаточно полного списка угроз;
– правильное указание на способы нейтрализации угроз.

Оценка «зачтено» ставится, если ответ в значительной степени соответствует перечисленным критериям оценивания.

Оценка «не зачтено» ставится, если ответ в большей степени или в целом не соответствует перечисленным критериям оценивания.

Контрольная работа

Описание технологии проведения

Обучающимся предлагается составить политику информационной безопасности для учебной лаборатории (компьютерного класса). Задание выполняется в течение 2 часов в письменном виде.

Требования к выполнению заданий, шкалы и критерии оценивания

Оценивание проводится по двухбалльной системе. Критерии оценивания включают в себя:
– системный и методический подход к созданию политики информационной безопасности;
– наличие достаточно полного списка угроз;
– правильное указание на способы нейтрализации угроз;
– аргументированность при выборе определенных правил политики.

Оценка «зачтено» ставится, если ответ в значительной степени соответствует перечисленным критериям оценивания.
Оценка «не зачтено» ставится, если ответ в большей степени или в целом не соответствует перечисленным критериям оценивания.

20.2 Промежуточная аттестация
Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:
Устный опрос.

Список вопросов:

1. Системный подход к обеспечению технологического процесса работы редакции конвергентного СМИ.
2. Технологические процессы редакции конвергентного СМИ.
3. Основное оборудование для обеспечения технологического процесса работы редакции конвергентного СМИ.
4. Основное программное обеспечение работы редакции конвергентного СМИ.
5. Политика редакционной информационной безопасности.
6. Технические средства обеспечения информационной безопасности редакции.
7. Доменные имена сайтов, их делегирование.
8. Хостинг, виды хостинга и требования к хостингу сайта СМИ.
9. Системы управления контентом.
9. Сервисы для обеспечения совместной работы.
10. Индивидуальные технические средства обеспечения работы корреспондента.
11. Основные угрозы информационной безопасности.
12. Программное обеспечение и сервисы для усиления информационной безопасности.

Описание технологии проведения

Каждый обучающийся получает КИМ (экзаменационный билет) с двумя вопросами и готовит по ним устный ответ. На подготовку ответов на КИМ дается 30 минут.

Требования к выполнению заданий, шкалы и критерии оценивания

Для оценивания результатов обучения используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».
Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует достаточно полные знания по темам вопросов, использует теоретические познания, практические навыки, собственный опыт	Повышенный уровень	Отлично
Обучающийся демонстрирует достаточно полные знания по темам вопросов, использует теоретические познания, практические навыки, собственный опыт, но его ответ содержит незначительные погрешности	Базовый уровень	Хорошо
Обучающийся демонстрирует знания по темам вопросов, использует теоретические познания, практические навыки, но его ответ недостаточно полный или содержит несколько ошибок	Пороговый уровень	Удовлетворительно
Обучающийся демонстрирует фрагментарные знания по темам вопросов, допускает значительные ошибки или дает неправильные ответы	–	Неудовлетворительно

Задания для диагностической работы

1. работы по информационной безопасности начинаются с:
а) аудита (верно);
б) выбора программного обеспечения;
в) закупки оборудования;
г) составления бизнес-плана.

2. Выберите из предложенных наиболее безопасный пароль:
а) 2128806;
madagaskar;
df5G6h4f&svG!; (верно)
Win6619.

3. Какой из вариантов хранения паролей наименее безопасен?
а) документ в облачном хранилище;
б) защищенная заметка в телефоне;
в) менеджер паролей в браузере; (верно)
г) отдельное приложение - менеджер паролей.

4. Срок делегирования доменного имени составляет:
а) любой, по желанию пользователя;
б) 1 месяц;
в) полгода;

г) 1 год. (верно)

5. Услуга по размещению сайта на веб-сервере называется ... (вставьте слово в именительном падеже).
Ответ: хостинг.

6. Вставьте пропущенное слово.
Домен типа jour.vsu.ru называется доменом ... уровня.
Ответ: третьего.

7. Вставьте пропущенное слово (прописью, не цифрами).
Резервное копирование данных обычно проводят ... раз в сутки.
Ответ: один.