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

УТВЕРЖДАЮ

Заведующий кафедрой
журналистики и литературы

Гордеев Ю. А.

16.12.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.03 Информационная безопасность в медиапроизводстве

1. Код и наименование направления подготовки: 42.04.02 Журналистика

2. Профиль 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: Научно-методическим советом факультета журналистики 16.12.2021 г. протокол № 4

8. Учебный год: 2023-2024 **Курс(ы):** 2

9. Цели и задачи учебной дисциплины

Целями учебной дисциплины являются:

– формирование у будущих специалистов и руководителей системных знаний по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками;

– формирование практических навыков безопасной работы в информационных системах.

Задачи учебной дисциплины:

– формирование системных представлений об управлении информационными рисками;

– изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;

– формирование практических навыков анализа защищенности информационных систем, использования встроенных возможностей ОС, MS Office, Брандмауэра Windows, Internet Explorer, а также антивирусных и криптографических средств для обеспечения безопасности информации;

– получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;

– изучение проблем защиты информации, стоящих перед современной вычислительной техникой;

– формирование навыков использования полученных знаний для правильного выбора решений при разработке криптографических, организационных, технических средств защиты информации.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина относится к обязательной части блока Б1 (Дисциплины (модули)) рабочего 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 компьютерами и смартфонами на уровне пользователя;

– навыки работы с офисными приложениями.

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	ОПК-6.1	Отслеживает глобальные тенденции модернизации технического оборудования, программного обеспечения и расходных материалов, необходимых для осуществления профессиональной	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, принципы создания политики безопасности. Уметь: оценивать угрозы для информационной безопасности.

	технологии		деятельности	Владеть: навыками действий для минимизации угроз для информации, навыками создания политики информационной безопасности офиса.
		ОПК-6.2	Адаптирует возможности новых стационарных и мобильных цифровых устройств к профессиональной деятельности журналиста	Знать: принципы работы стационарных и мобильных цифровых устройств к профессиональной деятельности журналиста. Уметь: отбирать и внедрять в профессиональную деятельность современные технологии рекламы и связей с общественностью, цифровые инструменты, технические средства и программное обеспечение. Владеть: приложениями и сервисами, обеспечивающими безопасность информации, хранящейся на электронных носителях, в веб-ресурсах, передающейся по различным каналам связи.
ПК-3	способен создавать концепцию и планировать реализацию индивидуального и (или) коллективного проекта (в том числе научно-исследовательского) в сфере медиа	ПК-3.1	Проводит многофакторный анализ перспектив запуска проекта в медиасфере	Знать: границы охвата политики информационной безопасности в зависимости от условий функционирования СМИ. Уметь: оценивать эффективность и анализировать результаты внедрения политики информационной безопасности редакции СМИ. Владеть: методами аудита и сбора информации для составления политики информационной безопасности редакции СМИ.

12. Объем дисциплины в зачетных единицах/час.: 3/108.

Форма промежуточной аттестации: экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость		
	Всего	По семестрам	
		Курс 2	Курс 2

			Сессия 1	Сессия 2
Аудиторные занятия		12	2	10
в том числе:	лекции	6	2	4
	практические	6	–	6
Самостоятельная работа		87	34	53
Форма промежуточной аттестации – экзамен		9	–	9
Итого:		108	36	72

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 телефоны. Основные угрозы для информационной безопасности. Техногенные и природные угрозы. Фишинг. Вирусы. Перехват информации. Атаки на сайт.	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
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.	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
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.	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
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	Информационная безопасность в медиасфере // Электронный

		копирования.	университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
2.2	Создание безопасных паролей	Способы взлома паролей. Методы противостояния взлому паролей. Требования к безопасному паролю.	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
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.	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962

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	2	–	14	16
2	Методы укрепления информационной безопасности	2	–	14	16
3	Технологии и методики безопасной коммуникации	2	–	14	16
4	Программное обеспечение для защиты информации	–	2	14	16
5	Создание безопасных паролей	–	2	14	16
6	Проведение онлайн-конференций и организация совместной удаленной работы	–	2	17	19
	Итого:	6	6	87	108 (включая 9 ч. промеж. аттестац.)

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 информацион- ной деятельности: учебное пособие. - Москва: ФЛИНТА, 2017. - URL: https://biblioclub.ru/index.php?page=book_red&id=482239.

б) дополнительная литература:

№ п/п	Источник
3	Шунейко, А. А. Информационная безопасность человека : учебное пособие : [16+] / А. А. Шунейко, И. А. Авдеенко. – Москва : Владос, 2018. – 177 с. : ил. – (Учебник для вузов (бакалавриат)). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=573372 . – Библиогр. в кн. – ISBN 978-5-906992-91-8. – Текст : электронный.
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.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
5	Электронная библиотека ЗНБ ВГУ. – Режим доступа: https://lib.vsu.ru/
6	ЭБС Университетская библиотека online. – Режим доступа: https://biblioclub.ru/
7	ЭБС «Лань». – Режим доступа: https://e.lanbook.com/
8	Информационная безопасность в медиасфере // Электронный университет. – URL: https://edu.vsu.ru/course/view.php?id=9962
	Security in a Box. Инструменты и рекомендации по цифровой безопасности. – URL: https://securityinabox.org/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/
3	Шунейко, А. А. Информационная безопасность человека : учебное пособие : [16+] / А. А. Шунейко, И. А. Авдеенко. – Москва : Владос, 2018. – 177 с. : ил. – (Учебник для вузов (бакалавриат)). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=573372 . – Библиогр. в кн. – ISBN 978-5-906992-91-8. – Текст : электронный.

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 Acdm; OfficeSTd 2013 RUS OLP NL Acdmc; Неисключительные права на ПО Dr. Web Enterprise Security Suite Комплексная защита Dr. Web Desktop Security Suite; СПС «ГАРАНТ- Образование».

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 Acdm; OfficeSTd 2013 RUS OLP NL Acdmc; Неисключительные права на ПО Dr. Web Enterprise Security Suite Комплексная защита Dr. Web Desktop Security Suite; СПС «ГАРАНТ- Образование».

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 Acdm; OfficeSTd 2013 RUS OLP NL Acdmc; Неисключительные права на ПО Dr. Web Enterprise Security Suite Комплексная защита Dr. Web Desktop Security Suite; СПС «ГАРАНТ- Образование».

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
2	Методы укрепления информационной беопасности	ОПК-6, ПК-3	ОПК-6.1, ОПК- 6.2, ПК-3.1	Контрольная работа

3	Технологии и методики безопасной коммуникации	ОПК-6, ПК-3	ОПК-6.1, ОПК-6.2, ПК-3.1	Опрос
4	Программное обеспечение для защиты информации	ОПК-6, ПК-3	ОПК-6.1, ОПК-6.2, ПК-3.1	Практическое задание
5	Создание безопасных паролей	ОПК-6, ПК-3	ОПК-6.1, ОПК-6.2, ПК-3.1	Практическое задание
6	Проведение онлайн-конференций и организация совместной удаленной работы	ОПК-6, ПК-3	ОПК-6.1, ОПК-6.2, ПК-3.1	Практическое задание
Промежуточная аттестация форма контроля – экзамен				Перечень вопросов

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:

Примерный перечень вопросов к экзамену:

Системный подход к обеспечению технологического процесса работы редакции конвергентного СМИ.

Технологические процессы редакции конвергентного СМИ.

Основное оборудование для обеспечения технологического процесса работы редакции конвергентного СМИ.

Основное программное обеспечение работы редакции конвергентного СМИ.

Политика редакционной информационной безопасности.

Технические средства обеспечения информационной безопасности редакции.

Доменные имена сайтов, их делегирование.

Хостинг, виды хостинга и требования к хостингу сайта СМИ.

Системы управления контентом.

Сервисы для обеспечения совместной работы.

Индивидуальные технические средства обеспечения работы корреспондента.

Основные угрозы информационной безопасности.

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