

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ МАССМЕДИА

ФАКУЛЬТЕТ ЖУРНАЛИСТИКИ

Кафедра телевизионных, радио- и интернет-технологий

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТ-СРЕДЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 42.03.02 - Журналистика

Направленность (профиль)- Мультимедийная журналистика и
современные медиатехнологии

Уровень квалификации выпускника: бакалавр

Форма обучения: очная, заочная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2019

Информационная безопасность в интернет-среде

Рабочая программа дисциплины

Составитель: Кандидат филологических наук Корнев М.С.

УТВЕРЖДЕНО

Протокол заседания кафедры ТРИТ

№__10/1__от 27.08.2019

ОГЛАВЛЕНИЕ

- 1 Пояснительная записка**
 - 1.1** Цель и задачи дисциплины
 - 1.2** Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине
 - 1.3** Место дисциплины в структуре образовательной программы
- 2 Структура дисциплины**
- 3 Содержание дисциплины**
- 4 Образовательные технологии**
- 5 Оценка планируемых результатов обучения**
 - 5.1** Система оценивания
 - 5.2** Критерии выставления оценок
 - 5.3** Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине
- 6 Учебно-методическое и информационное обеспечение дисциплины**
 - 6.1** Список источников и литературы
 - 6.2** Перечень ресурсов информационно-телекоммуникационной сети «Интернет»
- 7 Материально-техническое обеспечение дисциплины**
- 8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья**
- 9 Методические материалы**
 - 9.1** Планы практических (семинарских, лабораторных) занятий
 - 9.2** Методические рекомендации по подготовке письменных работ
 - 9.3** Иные материалы
- Приложения**
 - Приложение 1. Аннотация дисциплины
 - Приложение 2. Лист изменений

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цели и задачи дисциплины

Дисциплина «Информационная безопасность в интернет-среде» входит в состав вариативной части учебного плана бакалавриата по направлению подготовки 42.03.02 Журналистика.

Цель дисциплины – заложить методически и практически обоснованные знания, необходимые будущим специалистам по цифровым медиакоммуникациям, в области информационной безопасности и защиты информации

Задачи дисциплины:

- изучить терминологию и основные понятия теории защиты информации, нормативные документы и методы защиты компьютерной информации,
- дать представления о тенденциях развития информационной защиты с моделями возможных угроз,
- рассмотреть гуманитарный аспект в защите информации и человеческий фактор в сфере угроз информационной безопасности.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-2. Способен участвовать в производственном процессе выпуска журналистского текста и (или) продукта с применением современных редакционных технологий	ПК-2.1. Знает этапы производственного процесса выпуска журналистского текста и (или) продукта	<p>Знать: Терминологию и основные понятия теории защиты информации, нормативные документы.</p> <p>Уметь: Ориентироваться в современных аппаратно-программных решениях по защите информации.</p> <p>Владеть: Основными принципами и логикой проектирования систем защиты информации и критической инфраструктуры.</p>
	ПК-2.2. Использует современные редакционные технологии, медиаканалы и платформы в процессе выпуска журналистского текста	<p>Знать: Методы и средства защиты компьютерной информации. Психологические особенности в сфере организации и обеспечения информационной безопасности.</p> <p>Уметь: Выявлять источники, риски и формы атак на информацию, разрабатывать политику компании в</p>

	и (или) продукта	соответствии со стандартами безопасности. Проектировать многоуровневую защиту как корпоративных сетей и критической инфраструктуры организации, так и частных ИС. Владеть: Психологическими приемами противодействия социальным инженерам и манипуляторам
--	------------------	---

1.3 Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность в интернет-среде» относится к части, формируемой участниками образовательных отношений учебного плана. Изучение дисциплины базируется на знаниях, умениях и компетенциях студентов, полученных при освоении дисциплин «Техника и технология СМИ», «Создание мультимедийного ресурса», «Технологии работы с социальными медиа», «Мультимедийная журналистика», «Теория и практика новых медиа», «Профессионально-ознакомительная практика», «Профессионально-творческая практика».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Информационно-аналитическое обеспечение и планирование мультимедийного контента», «Журналистика глазами журналиста», «Взаимодействие служб по связям с общественностью и мультимедийного журналиста», «Преддипломная практика».

2. СТРУКТУРА ДИСЦИПЛИНЫ

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 44 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Актуальность	7	2		4			10	

	информационной безопасности, понятия и определения.								
2	Угрозы информационной безопасности	7	2		6			12	Тестирование
3	Гуманитарный аспект и человеческий фактор в информационной безопасности	7	2		4			10	
4	Методы и средства защиты информации и обеспечения информационной безопасности	7	2		6			12	Контрольная работа
5	Промежуточная аттестация: <i>Зачет</i>								По билетам
	итого:		8		20			44	72

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№	Наименование раздела дисциплины	Содержание
1	Актуальность информационной безопасности, понятия и определения.	Актуальность ИБ. Понятия и определения в информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Классификация и способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet.
2	Угрозы информационной безопасности	Виды угроз ИБ. Источники угроз ИБ. Условия существования вредоносных программ.
3	Гуманитарный аспект и человеческий фактор в информационной безопасности	Социальная инженерия. Психологические манипуляции. Агрессия в сети. Информационные войны.
4	Методы и средства защиты информации и обеспечения информационной безопасности	Методы и средства защиты компьютерной информации. Защита от компьютерных вирусов. Криптографические методы информационной безопасности. Критерии безопасности информационных систем.

4. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Наименование темы	Виды учебной работы	Образовательные технологии
1	Актуальность информационной безопасности, понятия и определения.	Лекция 1 Практические занятия 1-2 Самостоятельная работа	Лекция-визуализация с применением слайд-проектора. Развернутая беседа. Консультация
2	Угрозы информационной безопасности	Лекция 2 Практические занятия 3-5 Самостоятельная работа	Лекция-визуализация с применением слайд-проектора. Развернутая беседа. Консультация
3	Гуманитарный аспект и человеческий фактор в информационной безопасности	Лекция 3 Практические занятия 6-7 Самостоятельная работа	Лекция-визуализация с применением слайд-проектора. Развернутая беседа. Консультация
4	Методы и средства защиты информации и обеспечения информационной безопасности	Лекция Практические занятия 8-10 Самостоятельная работа	Лекция-визуализация с применением слайд-проектора. Развернутая беседа. Консультация

5. ОЦЕНКА ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
<i>Тестирование</i>	<i>20 баллов</i>	<i>20 баллов</i>
<i>Контрольная работа</i>	<i>40 баллов</i>	<i>40 баллов</i>
Промежуточная аттестация: зачет		<i>40 баллов</i>
Итого за семестр		<i>100 баллов</i>

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная	Традиционная шкала	Шкала
--------------	--------------------	-------

шкала			ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ А, В	«отлично»/ «зачтено (отлично)»/ «зачтено»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ С	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D, E	«удовлетвори- тельно»/ «зачтено (удовлетвори- тельно)»/ «зачтено»	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		учёт результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Оценочные материалы для текущего контроля успеваемости по дисциплине

Примерный вариант теста (ПК-2.1,2.2):

1. Общее определение термина «информационная безопасность»:

- а) состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры
- б) состояние беззащитности национальных интересов в информационной сфере, определяющихся совокупностью разбалансированных интересов личности, общества и государства
- в) атака на внешние и внутренние угрозы для национальных информационных ресурсов и государственных информационных систем, а так же телекоммуникационной инфраструктуры, организаций и служб

2. Понятие «кибербезопасность» шире, чем «информационная безопасность»?

- а) да

б) нет

3. «Информационная безопасность» как деятельность – это:

а) прогресс

б) процесс

в) результат

4. **Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности?

а) да

б) нет

5. Что обозначает аббревиатура «ИБ»:

а) история болезни

б) истребитель безотказный

в) информационная безопасность

6. Три ключевых аспекта при разработке системы ИБ:

а) технический (программный), правовой (законодательный), гуманитарный (административный)

б) быстрый, умеренный, медленный

в) красный, желтый, зеленый

7. Международный день защиты информации празднуется:

а) 12 декабря

б) 8 июня

в) 30 ноября

г) нет такого праздника

8. К системам «поддерживающей инфраструктуры» можно отнести:

а) системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций, обслуживающий персонал

б) кофе, чай, алкоголь и прочие психоактивные вещества

в) пандусы, ступеньки, перила, дверные ручки

9. Три ключевых характеристики состояния защищенности информации:

а) энергия, сила, ускорение

б) надежность, экономичность, качество

в) конфиденциальность, целостность, доступность

10. **К правовым методам, обеспечивающим информационную безопасность, относятся:**

а) Разработка аппаратных средств обеспечения правовых данных

б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий

в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Критерии оценки тестирования: каждый правильный ответ – 2 балла. Итого - 20 баллов максимум.

Примерные вопросы к контрольной работе (ПК-2.1,2.2):

1. Особенности современных информационных технологий?
 2. Классификация компьютерных преступлений?
 3. Экономические компьютерные преступления?
 4. Способы совершения компьютерных преступлений?
 5. Методы перехвата компьютерной информации?
 6. Пользователи и злоумышленники в Internet?
 7. Защита информации это?
 8. Угрозы безопасности информационных и телекоммуникационных средств и систем?
 9. Классификация угроз безопасности информации?
 10. Макровирусы.
 11. Спам? Основные виды спама.
 12. Антивирусные программы. Виды антивирусных программ.
 13. Методы обеспечения информационной безопасности Российской Федерации.
 14. Криптографические методы информационной безопасности. Классификация методов криптографического закрытия информации?
 15. Лицензирование и сертификация в области защиты информации?

Критерии оценки письменной контрольной работы:

31-40 баллов – оценка соответствует повышенному уровню и выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы

21-30 баллов - оценка соответствует повышенному уровню и выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос

11-20 баллов - оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.

0-10 баллов - оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки.

Оценочные материалы для промежуточной аттестации обучающихся по дисциплине (зачет)

Примерные вопросы к зачету (ПК-2.1,2.2):

1. Особенности современных информационных технологий и ИБ
2. Понятия «информационная безопасность» и «защита информации»
3. Особенности и различия понятий «информационная безопасность» и «кибер-безопасность»
4. Понятия «угрозы» ИБ, «уязвимости», «атака» и «злоумышленники»
5. Составляющие информационной безопасности: конфиденциальность, целостность, доступность
6. Различные подходы и масштабы информационной безопасности
7. Что понимается под информационной безопасностью Российской Федерации
8. Основные виды и способы преступлений, связанных с вмешательством в работу компьютеров?
9. Основные принципы и логика защиты информации
10. Какие факторы надо учитывать при проектировании системы ИБ?
11. В чем состоит комплексный подход при создании системы ИБ
12. В чем состоит модульный принцип при проектировании системы ИБ
13. Принцип «слабого звена» при проектировании системы ИБ
14. Понятие «приемлемого ущерба» и меры по защите информации
15. Основные принципы при формировании политики безопасности
16. Хакеры и социальные инженеры: основные угрозы и их предотвращение
17. Психология манипулирования и ИБ
18. Информационные войны и информационная безопасность
19. Уязвимость цифровых носителей и сети Интернет: угрозы и возможности
20. Аппаратные и программные средства защиты информации

35-40 баллов – оценка соответствует повышенному уровню и выставляется обучающемуся, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы

29-34 баллов - оценка соответствует повышенному уровню и выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос

20-28 баллов - оценка соответствует пороговому уровню и выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.

0-20 баллов - оценка выставляется обучающемуся, который не достигает порогового уровня, демонстрирует непонимание проблемы, не знает значительной части программного материала, допускает существенные ошибки.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Список источников и литературы

Источники

1. Закон Российской Федерации от 27.12.1991 №2124-1 «О средствах массовой информации» (действующая редакция от 24.11.2014)
2. О сертификации продукции и услуг/ Закон Российской Федерации
3. О федеральных органах правительственной связи и информации/ Закон Российской Федерации
4. О государственной тайне/ Закон Российской Федерации
5. Об информации, информатизации и защите информации/ Закон Российской Федерации

Литература

Основная

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>

2. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449779>
3. Трофимов, В. В. Информационные технологии в 2 т. Том 1 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 238 с. — (Высшее образование). — ISBN 978-5-534-01935-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451790>
4. Трофимов, В. В. Информационные технологии в 2 т. Том 2 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 390 с. — (Высшее образование). — ISBN 978-5-534-01937-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451791>

Дополнительная

1. Калмыков, А.А. Интернет-журналистика: Учеб. пособие для студентов вузов, обучающихся по специальности 021400 «Журналистика» / А.А. Калмыков, Л.А. Коханова. — М. : ЮНИТИ-ДАНА, 2017. — 383 с. — (Серия «Медиаобразование»). - ISBN 978-5-238-00771-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1028746>
2. Алтунян, А. Г. От «глобальной деревни» к «информационным хуторам». Журналистика в эпоху перемен : монография / А. Г. Алтунян. - Монография : Университетская книга, 2019. - 308 с. - ISBN 978-5-98699-312-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1213098>

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационная безопасность и защита информации (курс лекций) - <http://www.mylect.ru/informatic/securityinformation.html>
2. Сайт COSSA.RU - www.cossa.ru
3. Сайт BESTAPP - <http://bestapp.menu/>
4. Сайт «Мы и Жо» - <http://themedia.center/>
5. Сайт Постжурналист - <http://postjournalist.ru/>
6. Сайт АКА-МЕДИА - <http://www.aka-media.ru/>
7. Сообщество и блог MediaToolBox - <https://www.facebook.com/mdtlbx>
<http://mediatoolbox.ru/blog/>

8. Дискуссионная платформа "Новые медиа в гуманитарном образовании»
(группа в Facebook) - <https://www.facebook.com/groups/newmediaedu/>

Перечень БД и ИСС

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение дисциплины базируется на ресурсах любого класса, укомплектованного мультимедийным проектором, компьютером и экраном, доской.

Операционная система Microsoft Windows 7, 10 Pro, Microsoft Office 2010, 2013, 2016, Kaspersky Endpoint Security, WinRAR : 4, Acrobat Professional 9

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
 - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
 - для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере со специализированным программным обеспечением;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
 - в форме аудиофайла.
- для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа;
 - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
 - устройством для сканирования и чтения с камерой SARA CE;
 - дисплеем Брайля PAC Mate 20;
 - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
 - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
 - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
 - передвижными, регулируемые эргономическими партами СИ-1;
 - компьютерной техникой со специальным программным обеспечением.

9. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

9.1. Планы практических занятий.

Тема 1. Актуальность информационной безопасности, понятия и определения. (4 ч.)

Цель занятия: закрепление знаний об основных понятиях и определениях, актуальных проблемах ИБ

Форма проведения – дискуссия

Вопросы для обсуждения:

1. Актуальность ИБ. Понятия и определения в информационной безопасности.
2. Национальные интересы РФ в информационной сфере и их обеспечение.
3. Классификация и способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet.

Контрольные вопросы:

1. Дайте определение понятию информационная безопасность.
2. Перечислите основные составляющие информационной безопасности.
3. Какое значение имеют составляющие информационной безопасности для субъектов информационных отношений?
4. Каковы интересы РФ в информационной сфере?

Рекомендуемая литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449779>
3. Трофимов, В. В. Информационные технологии в 2 т. Том 1 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 238 с. — (Высшее образование). — ISBN 978-5-534-01935-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451790>
4. Трофимов, В. В. Информационные технологии в 2 т. Том 2 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 390 с. — (Высшее образование). — ISBN 978-5-534-01937-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451791>

Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Научный журнал «Медиаскоп» - www.mediascope.ru

2. Информационная безопасность и защита информации (курс лекций) - <http://www.mylect.ru/informatic/securityinformation.html>
3. Сайт COSSA.RU - www.cossa.ru
4. Сайт BESTAPP - <http://bestapp.menu/>
5. Сайт «Мы и Жо» - <http://themedia.center/>
6. Сайт Постжурналист - <http://postjournalist.ru/> Сайт АКА-МЕДИА - <http://www.aka-media.ru/>
7. Сообщество и блог MediaToolBox - <https://www.facebook.com/mdtlbx>
<http://mediatoolbox.ru/blog/>
8. Дискуссионная платформа "Новые медиа в гуманитарном образовании» (группа в Facebook) - <https://www.facebook.com/groups/newmediaedu/>

Тема 2. Угрозы информационной безопасности (6 ч.)

Цель занятия: закрепление знаний об угрозах ИБ в их разных формах и проявлениях

Форма проведения – дискуссия

Вопросы для обсуждения:

1. Виды угроз ИБ. Источники угроз ИБ.
2. Условия существования вредоносных программ.

Контрольные вопросы:

1. Определите источники угроз ИБ и постройте их классификацию.
2. Перечислите основные методы обеспечения ИБ

Рекомендуемая литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449779>
3. Трофимов, В. В. Информационные технологии в 2 т. Том 1 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 238 с. — (Высшее образование). — ISBN 978-5-534-01935-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451790>

4. Трофимов, В. В. Информационные технологии в 2 т. Том 2 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 390 с. — (Высшее образование). — ISBN 978-5-534-01937-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451791>

Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Научный журнал «Медиаскоп» - www.mediascope.ru
2. Информационная безопасность и защита информации (курс лекций) - <http://www.mylect.ru/informatic/securityinformation.html>
3. Сайт COSSA.RU - www.cossa.ru
4. Сайт BESTAPP - <http://bestapp.menu/>
5. Сайт «Мы и Жо» - <http://themedia.center/>
6. Сайт Постжурналист - <http://postjournalist.ru/> Сайт АКА-МЕДИА - <http://www.aka-media.ru/>
7. Сообщество и блог MediaToolBox - <https://www.facebook.com/mdtlbx>
<http://mediatoolbox.ru/blog/>
8. Дискуссионная платформа "Новые медиа в гуманитарном образовании" (группа в Facebook) - <https://www.facebook.com/groups/newmediaedu/>

Тема 3. Гуманитарный аспект и человеческий фактор в информационной безопасности (4 ч.)

Цель занятия: Изучение и обсуждение гуманитарного измерения и роли человеческого фактора в информационной безопасности.

Форма проведения – дискуссия, доклады.

Вопросы для обсуждения:

1. Социальная инженерия. Психологические манипуляции.
2. Агрессия в сети. Информационные войны.

Контрольные вопросы:

1. Методы воздействия и противодействия социальной инженерии и психологическим манипуляциям
2. Проблема digital-агрессии: кто виноват и что делать? Информационные войны в медиaprостранстве.

Рекомендуемая литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. —

- 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449779>
3. Трофимов, В. В. Информационные технологии в 2 т. Том 1 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 238 с. — (Высшее образование). — ISBN 978-5-534-01935-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451790>
4. Трофимов, В. В. Информационные технологии в 2 т. Том 2 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 390 с. — (Высшее образование). — ISBN 978-5-534-01937-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451791>

Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Научный журнал «Медиаскоп» - www.mediascope.ru
2. Информационная безопасность и защита информации (курс лекций) - <http://www.mylect.ru/informatic/securityinformation.html>
3. Сайт COSSA.RU - www.cossa.ru
4. Сайт BESTAPP - <http://bestapp.menu/>
5. Сайт «Мы и Жо» - <http://themedia.center/>
6. Сайт Постжурналист - <http://postjournalist.ru/> Сайт АКА-МЕДИА - <http://www.aka-media.ru/>
7. Сообщество и блог MediaToolBox - <https://www.facebook.com/mdtlbx>
<http://mediatoolbox.ru/blog/>
8. Дискуссионная платформа "Новые медиа в гуманитарном образовании" (группа в Facebook) - <https://www.facebook.com/groups/newmediaedu/>

Тема 4. Методы и средства защиты информации и обеспечения информационной безопасности (6 ч.)

Цель занятия: Изучение и обсуждение методов и средств защиты информации

Форма проведения – дискуссия

Вопросы для обсуждения:

1. Методы и средства защиты компьютерной информации. Критерии безопасности информационных систем.
2. Защита от компьютерных вирусов. Криптографические методы ИБ.

Контрольные вопросы:

1. Сформулировать основные принципы построения системы защиты информации.
2. Перечислить основные модели защиты информации и их особенности.

Рекомендуемая литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449285>
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449779>
3. Трофимов, В. В. Информационные технологии в 2 т. Том 1 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 238 с. — (Высшее образование). — ISBN 978-5-534-01935-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451790>
4. Трофимов, В. В. Информационные технологии в 2 т. Том 2 : учебник для вузов / В. В. Трофимов ; ответственный редактор В. В. Трофимов. — Москва : Издательство Юрайт, 2020. — 390 с. — (Высшее образование). — ISBN 978-5-534-01937-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451791>

Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. Научный журнал «Медиаскоп» - www.mediascope.ru
2. Информационная безопасность и защита информации (курс лекций) - <http://www.mylect.ru/informatic/securityinformation.html>
3. Сайт COSSA.RU - www.cossa.ru
4. Сайт BESTAPP - <http://bestapp.menu/>
5. Сайт «Мы и Жо» - <http://themedia.center/>
6. Сайт Постжурналист - <http://postjournalist.ru/> Сайт АКА-МЕДИА - <http://www.aka-media.ru/>
7. Сообщество и блог MediaToolBox - <https://www.facebook.com/mdtlbx>
<http://mediatoolbox.ru/blog/>

8. Дискуссионная платформа "Новые медиа в гуманитарном образовании» (группа в Facebook) - <https://www.facebook.com/groups/newmediaedu/>

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность в интернет-среде» реализуется на факультете журналистики кафедрой «Телевизионных, радио- и интернет технологий»

Цель дисциплины – заложить методически и практически обоснованные знания, необходимые будущим специалистам по цифровым медиакоммуникациям, в области информационной безопасности и защиты информации

Задачи дисциплины:

- изучить терминологию и основные понятия теории защиты информации, нормативные документы и методы защиты компьютерной информации,
- дать представления о тенденциях развития информационной защиты с моделями возможных угроз,
- рассмотреть гуманитарный аспект в защите информации и человеческий фактор в сфере угроз информационной безопасности.

Дисциплина направлена на формирование следующих компетенций:

ПК-2. Способен участвовать в производственном процессе выпуска журналистского текста и (или) продукта с применением современных редакционных технологий

В результате освоения дисциплины обучающийся должен:

Знать: Терминологию и основные понятия теории защиты информации, нормативные документы; методы и средства защиты компьютерной информации. Психологические особенности в сфере организации и обеспечения информационной безопасности.

Уметь: Ориентироваться в современных аппаратно-программных решениях по защите информации; выявлять источники, риски и формы атак на информацию, разрабатывать политику компании в соответствии со стандартами безопасности. Проектировать многоуровневую защиту как корпоративных сетей и критической инфраструктуры организации, так и частных ИС.

Владеть: Основными принципами и логикой проектирования систем защиты информации и критической инфраструктуры; психологическими приемами противодействия социальным инженерам и манипуляторам

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	Приложение №1	31.08.2020	10

1. Структура дисциплины (к п. 2 на 2020 г.)**Структура дисциплины для очной формы обучения**

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 48 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Актуальность информационной безопасности, понятия и определения.	7	2		4			12	
2	Угрозы информационной безопасности	7	2		6			12	Тестирование
3	Гуманитарный аспект и человеческий фактор в информационной безопасности	7	2		4			12	
4	Методы и средства защиты информации и обеспечения информационной безопасности	7	2		6			12	Контрольная работа
5	Промежуточная аттестация: Зачет								По билетам
	итога:		8		20			48	76

Структура дисциплины для заочной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 76 ч., в том числе контактная работа обучающихся с преподавателем 8 ч., самостоятельная работа обучающихся 68 ч.

№ п/п	Раздел дисциплины/темы	курс	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Актуальность информационной безопасности, понятия и определения.	4	2					17	
2	Угрозы информационной безопасности	4	2		1			17	Тестирование
3	Гуманитарный аспект и человеческий фактор в информационной безопасности	4	1					17	
4	Методы и средства защиты информации и обеспечения информационной безопасности	4	1		1			17	Контрольная работа
5	Промежуточная аттестация: <i>Зачет</i>								По билетам
	итога:		6		2			68	76

2. Образовательные технологии (к п.4 на 2020 г.)

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

3. Перечень БД и ИСС (к п. 6.2 на 2020 г.)

№п /п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

4. Состав программного обеспечения (ПО) (к п. 7 на 2020 г.)

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	лицензионное
7	Microsoft Office 2016	Microsoft	лицензионное
8	Zoom	Zoom	лицензионное

