МИНОБРНАУКИ РОССИИ

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

ИНСТИТУТ МАССМЕДИА И РЕКЛАМЫ

ФАКУЛЬТЕТ ЖУРНАЛИСТИКИ

Кафедра телевизионных, радио- и интернет-технологий

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ВИЗУАЛЬНЫХ МЕДИА

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 42.03.02 - Журналистика

Направленность (профиль) – Современные визуальные медиа

Уровень высшего образования: *бакалавриат*

Форма обучения - очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

Информационная безопасность в визуальных медиа
Рабочая программа дисциплины
Составитель: Кандидат филологических наук Корнев М.С.

УТВЕРЖДЕНО

Протокол заседания кафедры ТРИТ

№ 2 от 01.03.2024 г.

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цели и задачи дисциплины

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	*Знать:* Методы и средства защиты компьютерной информации; терминологию и основные понятия теории защиты информации, *Уметь:* Ориентироваться в современных аппаратно-программных решениях по защите информации; разрабатывать политику компании в соответствии со стандартами безопасности *Владеть:* Основными принципами и логикой проектирования систем защиты информации и критической инфраструктуры; приемами защиты информации
	ПК-2.2. Использует современные редакционные технологии, медиаканалы и платформы в процессе выпуска журналистского текста и (или) продукта	*Знать:* нормативные документы *Уметь:* Выявлять источники, риски и формы атак на информацию; психологические особенности в сфере организации и обеспечения информационной 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 визуальных медиа» относится к части, формируемой участниками образовательных отношений части учебного плана. Изучение дисциплины базируется на знаниях, умениях и компетенциях студентов, полученных при освоении дисциплин и прохождения практик «Информационные технологии в медиасистеме», «Техника и технология СМИ», «Телевизионная режиссура», «Профессионально-творческая практика».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Журналистика глазами журналиста», «Актуальные проблемы современности в визуальных медиа», «Специфика деятельности журналиста на информационном канале».

2. СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
8	Лекции	10
	Практические занятия	32
Всего:		42

Объем дисциплины в форме самостоятельной работы обучающихся составляет 66 академических часов.

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№	Наименование раздела дисциплины	Содержание
1	Актуальность информационной	Актуальность ИБ. Понятия и определения в информационной безопасности. Национальные интересы

	безопасности, понятия и определения.	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

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. ОЦЕНКА ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *Тестирование* *Контрольная работа*	 *20 баллов* *40 баллов*	 *20 баллов* *40 баллов*
Промежуточная аттестация: зачет с оценкой		*40 баллов*
Итого за семестр *зачёт с оценкой*		*100 баллов*

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 шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично		A

83 – 94		зачтено	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/ A, B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. 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. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	«удовлетвори-тельно»/ «зачтено (удовлетвори-	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.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	тельно)»/ «зачтено»	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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом 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 выставляются 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:

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.

0-19 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 с оценкой)

Примерные вопросы к зачету с оценкой (ПК-2.1,2.2)

1. Особенностями 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»
1. Составляющие информационной безопасности: конфиденциальность, целостность, доступность
2. Различные подходы и масштабы информационной безопасности
5. Что понимается под информационной безопасностью Российской Федерации
6. Основные виды и способы преступлений, связанных с вмешательством в работу компьютеров?
3. Основные принципы и логика защиты информации
4. Какие факторы надо учитывать при проектировании системы ИБ?
1. В чем состоит комплексный подход при создании системы ИБ
7. В чем состоит модульный принцип при проектировании системы ИБ
8. Принцип «слабого звена» при проектировани системы ИБ
9. Понятие «приемлемого ущерба» и меры по защите информации
10. Основные принципы при формировании политики безопасности
11. Хакеры и социальные инженеры: основные угрозы и их предотвращение
12. Психология манипулирования и ИБ
13. Информационные войны и информационная безопасность

14. Уязвимость цифровых носителей и сети Интернет: угрозы и возможности
15. Аппаратные и программные средства защиты информации

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 средства 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

Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022

Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 - Режим доступа: http://znanium.com/bookread2.php?book=405000

Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133

Дополнительная

Борисова Ирина Валентиновна Цифровые методы обработки информации/БорисоваИ.В. - Новосиб.: НГТУ, 2014. - 139 с.: ISBN 978-5-7782-2448-3 - Режим доступа: http://znanium.com/catalog/product/546207

Попов, И. В. Информационная безопасность : практикум / И. В. Попов, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2022. - 90 с. - ISBN 978-5-91612-375-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2016193

Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Национальная электронная библиотека (НЭБ) www.rusneb.ru

ELibrary.ru Научная электронная библиотека www.elibrary.ru

Электронная библиотека Grebennikon.ru www.grebennikon.ru

Cambridge University Press

ProQuest Dissertation & Theses Global

SAGE Journals

Taylor and Francis

JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

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

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Adobe Master Collection

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, регулируемыми 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. (8 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?

Тема 2. Угрозы информационной безопасности (8 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

Тема 3. Гуманитарный аспект и человеческий фактор в информационной безопасности (8 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 психологически манипуляциям
2. Проблема digital-агрессии: кто виноват и что делать? Информационные войны в медиапространстве.

Тема 4. Методы и средства защиты информации и обеспечения информационной безопасности (8 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.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность в визуальных медиа» 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; приемами защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.