Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Алтайский филиал

УТВЕРЖДЕНО

Ученым советом
Алтайского филиала РАНХиГС

Протокол № 8 от 29 апреля 2021 года

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ

«Медиакоммуникации»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.08 Кибербезопасность

Магистр

42.04.05 Медиакоммуникации
Профиль «Медиаменеджмент и связи с общественностью в государственных и бизнес-структурах»

Заочная

Год набора – 2022

Барнаул, 2021 г.

Авторы–составители:

к.т.н., доцент кафедры гуманитарных и естественнонаучных дисциплин, доцент Лопухов В.М.

и.о. заведующего кафедрой медиакоммуникаций, русского языка и риторики, к.фил.н. Шмаков Артем Алексеевич

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Дисциплина Б1.О.08 «Кибербезопасность» обеспечивает овладение следующими:

Код Компетенции	Наименование компетенции	Код компонента и(или) этапа компетенции	Наименование компонента и(или) этапа компетенции
ОПК-6	способен отбирать и внедрять в процесс медиапроизводства современные технические средства и информационно-коммуникационные технологии	ОПК-6.1	Способен оценивать потенциальные риски и угрозы безопасности при осуществлении продвижения социально значимых проектов
		ОПК-6.2	Способен отслеживать глобальные тенденции модернизации технических средств и информационно-коммуникационных технологий для осуществления профессиональной деятельности

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ/трудовые или профессиональные действия	Код компонента компетенции	Результаты обучения
	ОПК-6.1	**на уровне знаний:** Знает основные возможные риски и угрозы, которые потенциально могут возникнуть в процессе продвижения социально значимых проектов.
		на уровне умений: Умеет прогнозировать риски и угрозы, которые потенциально могут возникнуть в процессе продвижения социально значимых проектов.
		на уровне навыков: Владеет навыками оценки потенциальных рисков и угроз безопасности при осуществлении продвижения социально значимых проектов.
	ОПК-6.2	**на уровне знаний:** Знает методы и средства защиты информации, необходимые для предупреждения правонарушений, выявления и устранения причин и условий совершения правонарушений в киберпространстве.
		на уровне умений: Умеет выявлять источники угроз кибербезопасности; применять знания нормативно-правовой базы по кибербезопасности к практическим ситуациям, связанным с предупреждением правонарушений, выявлением и устранением причин совершения правонарушений в киберпространстве.
		на уровне навыков: Владеет навыками применения подходов для выработки конкретных, научно-обоснованных предложений по правовому решению задач в сфере кибербезопасности.

2. Объем и место дисциплины в структуре ОП ВО

Общий объем дисциплины составляет – 2 з.е., 72 академических часов (54 астрономический час).

Количество астрономических и соответствующих им академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) на заочной форме обучения составляет 12 академических часа (9 астрономических часа), из них лекции – 4 академических часа (3 астрономических часа), практические занятия – 8 академических часа (6 астрономических часа), на самостоятельную работу обучающихся количество астрономических и соответствующих им академических часов составляет – 60 академических часа (45 астрономических часа).

Дисциплина Б1.О.08 «Кибербезопасность» относится к вариативной части и в соответствии с учебным планом осваивается в 3 (1 курс) и 4 семестре (2 курс) на заочной форме обучения.

Форма промежуточной аттестации в соответствии с учебным планом – зачёт.

3. Содержание и структура дисциплины (модуля)

Заочная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Концептуальная модель кибербезопасности	19	1		2		16	Т
Тема 2	Конфиденциальная информация в киберпространстве. Законодательство Российской Федерации о кибербезопасности	29	1		4		24	ТЗ, Т
Тема 3	Обеспечение кибербезопасности медиапроизводства	24	2		2		20	ДП
Промежуточная аттестация								Зачёт
Всего:		72	4		8		60	

Используемые сокращения:

Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся);

ЛР – лабораторные работы (вид занятий семинарского типа);

ПЗ – практические занятия (виды занятия семинарского типа за исключением лабораторных работ);

КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации);

ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.

СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях;

Т – Тест;

ТЗ – типовое задание;

ДП – доклад-презентация.

Содержание дисциплины (модуля)

№ п/п	Наименование тем (разделов)	Содержание тем (разделов)
1	Концептуальная модель кибербезопасности	Кибербезопасность как наука и научная дисциплина. Актуальность защиты информации. Терминология области защиты данных. Преступления в сфере компьютерной информации. Система защиты информации. Концептуальная модель кибербезопасности: угрозы информации, объекты угроз, цели злоумышленников, способы защиты информации, источники угроз, основные направления, средства защиты информации, действия, приводящие к неправомерному овладению конфиденциальной информацией. Модели области защиты данных. Направления обеспечения кибербезопасности: правовое, организационное и инженерно-техническое. Комплексный подход к разработке системы защиты информации. Противоправные действия с информацией. Угрозы кибербезопасности профессиональной деятельности. Классификация угроз и специфические виды угроз для компьютерных сетей. Цели, субъекты и уровни уязвимости кибербезопасности. Каналы утечки информации. Пути несанкционированного доступа к информации. Проектирование системы обеспечения кибербезопасности. Типовой порядок действий по обеспечению кибербезопасности. Использование информации в компьютерных сетях для совершения правонарушений и преступлений. Критерии безопасности компьютерных систем. Криптографическая защита. Электронная подпись. Разграничение доступа, ролевое управление доступом. Защита компьютерных систем. Идентификация и аутентификация. Компьютерные вирусы и вредоносное программное обеспечение. Восстановление данных. Анализ защищённости. Служба защиты информации и её организационно-методическая работа. Мониторинг информационного обмена

		и аудит действий пользователей в компьютере. Методы и средства физической, программной, аппаратной и криптографической защиты информации. Правила поведения в сети «Интернет» и «компьютерная гигиена». Преступления в «киберпространстве», «кибервойна». Принципы кибербезопасности. Экспертные группы, занимающиеся изучением инцидентов компьютерной безопасности. Предметные области кибербезопасности и ее субъекты.
2	Конфиденциальная информация в киберпространстве. Законодательство Российской Федерации о кибербезопасности	Доступ к информации, классификация информации по доступу к ней. Виды информации ограниченного доступа в медиапроизводстве. Правовое регулирование профессиональной тайны. Обеспечение профессиональной тайны. Правовое регулирование профессиональной тайны. Структура и состав организационно-правового обеспечения профессиональной тайны. Проблемы правовой ответственности в сфере профессиональной тайны. Обеспечение защиты персональных данных. Структура и состав организационно-правового обеспечения защиты персональных данных. Проблемы правовой ответственности в сфере персональных данных. Виды служебной и профессиональной тайн. Правовое регулирование служебной и профессиональной тайны. Объекты авторского и патентного права, их правовое регулирование. Структура информационного законодательства о кибербезопасности в Российской Федерации. Международное законодательства о кибербезопасности. Правовое обеспечение безопасности в информационной сфере. Государственные регуляторы в области кибербезопасности. Стандарты в сфере кибербезопасности. Защита прав граждан в информационной сфере. Государственная политика в сфере обеспечения кибербезопасности. Нормативные документы по кибербезопасности мебиапроизводства. Интернет как явление и процесс. Правовые проблемы Интернета. Нормативная правовая база по вопросам функционирования сети «Интернет» в России. Правовые аспекты обеспечения безопасности в Интернете. Ответственность за нарушение законодательства в области информационной безопасности. Современные проблемы кибербезопасности в России. Положительный опыт зарубежных государств в правовом обеспечении кибербезопасности.
3	Обеспечение кибербезопасности медиапроизводства	Противоправные действия с информацией в медиапроизводстве. Угрозы кибербезопасности медиапроизводства. Критическая информационная инфраструктура медиапроизводства. Использование информации в компьютерных сетях для совершения правонарушений и преступлений. Критерии безопасности компьютерных систем.

		Криптографическая защита. Электронная подпись. Экранирование, персональные и корпоративные межсетевые экраны, их назначение. Антивирусная защита. Разграничение доступа, ролевое управление доступом. Защита компьютерных систем. Идентификация и аутентификация, парольная аутентификация, идентификация/аутентификация с помощью биометрических данных. Правила выбора пароля. Сетевые вирусы. Правила поведения в сети «Интернет» и «компьютерная гигиена». Преступления в «киберпространстве». Кибербезопасность в «Интернет-вещей». «Умный дом» - риски и проблемы.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации

4.1.1. В ходе реализации дисциплины Б1.О.08 «Кибербезопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Тема и/или раздел	Методы текущего контроля успеваемости
Тема 1. Концептуальная модель кибербезопасности	Тест
Тема 2. Конфиденциальная информация в киберпространстве. Законодательство Российской Федерации о кибербезопасности	Тест, типовое задание
Тема 3. Обеспечение кибербезопасности медиапроизводства	Доклад-презентация

4.1.2. Зачёт проходит в виде устного опроса, а также учитывает результаты текущего контроля успеваемости обучающихся.

4.2. Материалы текущего контроля успеваемости обучающихся

Примерные оценочные материалы по Теме 1. Концептуальная модель кибербезопасности

Типовые вопросы теста по теме 1:

Вопрос 1. К какой группе средств относятся механические, электрические, электронные и др. устройства, предназначенные для защиты информации от утечки и разглашения, и противодействия техническим средствам промышленного шпионажа?

Варианты ответов:

1: аппаратные;
2: программные;
3: криптографические;
4: физические;
5: организационное;
6: правовое.

Вопрос 2. Ботнет - это ...

Варианты ответов:

1: Это компьютерная сеть (network), состоящая из некоторого количества хостов, с запущенными ботами (robot), т.е. автономным ПО;

2: Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей;

3: DDoS- атака, которая начинаются с чужого адреса, скрывающего хакера;

4: Внедрение сторонних данных или команд в систему с целью изменения хода работы системы и получения доступа к закрытым функциям и информации.

Вопрос 3. Миниатюрное электронное устройство перехвата речевой информации, состоящее из микрофона и радиопередатчика, обеспечивающего передачу подслушанного звукового сигнала на достаточно значительное расстояние с помощью электромагнитных волн, ЭТО?

Варианты ответов:

1: закладное подслушивающее устройство;

2: "жучок";

3: "паучок";

4: скремблер;

5: дешифратор;

6: криптофон;

7: радиозакладка.

Вопрос 4. Как расшифровывается аббревиатура «СЗИ» с точки зрения информационной безопасности?

Варианты ответов:

1: Система защиты информации;

2: Средства защиты интересов;

3: Способы запроса информации;

4: Способ защиты инноваций.

Вопрос 5. Выберите определение понятия «Угрозы конфиденциальной информации».

Варианты ответов:

1: Потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями;

2: Нарушение физической целостности уничтожением;

3: Нарушение логической структуры искажением структуры;

4: Нарушение содержания несанкционированной модификацией.

Вопрос 6. Вредоносная программа – это

1: Созданная или уже существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, систему ЭВМ или их сети;

2: Программа, которая выявляет, предотвращает и выполняет определенные действия, чтобы блокировать или удалять вредоносные программы, такие как вирусы и черви;

3: Программа, осуществляющая контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами;

4: Программа, предназначенная для увеличения производительности системы и ускорения ее работы.

Вопрос 7. К какой группе средств относятся устройства, передающие речь в цифровом и зашифрованном виде. Вместо собственно речевого сигнала они передают только значения его определённых параметров, которые на приемной стороне управляют синтезатором речи?

Варианты ответов:

1: маскираторы электромагнитных излучений и наводок;

2: скремблеры;

3: криптофоны;

4: маскираторы речи;

5: вокодеры;

6: преобразователи голоса.

Вопрос 8. Укажите правильные высказывания из области криптографии.

Варианты ответов:

1: сложность написания символов в шифре замены усложняет процесс "вскрытия" зашифрованного сообщения;

2: при "вскрытии" сообщения, зашифрованного шифром простой однобуквенной замены, подсчитывают частоты вхожения символов;

3: слово-лозунг используют для лёгкого запоминания ключа;

4: в шифре разнозначной замены одной букве могут ставится в соответствие один или два символа.

Вопрос 9. Укажите, для чего используется криптография.

Варианты ответов:

1: Для защиты конфиденциальности данных;

2: Для защиты целостности данных;

3: Для неотказуемости данных;

4: Для аутентичности данных.

Вопрос 10. Как называется информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Варианты ответов:

1: электронная подпись;

2: электронная цифровая подпись;

3: электронный документ;

4: хеш-функция.

Тема 2. Конфиденциальная информация в киберпространстве. Законодательство Российской Федерации о кибербезопасности

Типовое задание по теме 2:

1. Выберите конкретное, которое будет являться объектом исследования.
2. Дайте общее описание выбранного медиапроизводства.
3. Определите перечень сведений конфиденциального характера, обрабатываемых в выбранном медиапроизводстве и которую необходимо защищать.
4. Отсортируйте перечень сведений конфиденциального характера по значимости с указанием НПА, регламентирующих их защиту.
5. Определите отношение сотрудников к защищаемой информации (пользователь, владелец, собственник, др.).
6. Доложите о проделанной работе преподавателю на учебном занятии.

Типовые вопросы теста по теме 2:

Вопрос 1. ... - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)?

Выберите один ответ:

a. Информация личного характера;

b. Персональные данные;

c. Тайна;

d. Данные.

Вопрос 2. Блокирование ПДн - это …

Выберите один ответ:

a. временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных;

b. вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям;

c. вспомогательный процесс;

d. непрерывный процесс наблюдения и регистрации параметров объекта, в сравнении с заданными критериями.

Вопрос 3. Укажите виды конфиденциальной информации, связанной с хозяйственной деятельностью.

Выберите один или несколько ответов:

a. сведения, содержащие государственную тайну;
b. объекты патентного права;
c. персональные данные;
d. коммерческая тайна;
e. объекты авторского права;
f. общедоступная.

Вопрос 4. Укажите термин, к которому относится следующее определение:

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Выберите один ответ:

a. Компьютерная атака;
b. Показатель защищенности информации;
c. Техника защиты информации;
d. Защищаемый объект информатизации;
e. Политика безопасности;
f. Компьютерный инцидент.

Вопрос 5. Укажите виды тайн, выделенные в Указе Президента РФ от 06.03.1997 N 188 «Об утверждении перечня сведений конфиденциального характера».

a. Выберите один или несколько ответов:
b. Сведения, связанные с профессиональной деятельностью…
c. Сведения, составляющие тайну следствия и судопроизводства…
d. Сведения, связанные с коммерческой деятельностью… (коммерческая тайна).
e. Сведения о сущности изобретения, полезной модели или промышленного образца…
f. Сведения, содержащиеся в личных делах осужденных…

g. Служебные сведения, доступ к которым ограничен органами государственной власти… (служебная тайна).

h. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные) …

Вопрос 6. Выберите один или несколько ответов:

a. На лицах, которым доверена информация, не подлежащая оглашению, не лежит правовая обязанность ее хранить;

b. Сведения подлежат разглашению (огласке);

c. Тайна есть, прежде всего, сведения, информация;

d. Сведения должны быть известны или доверены узкому кругу лиц.

Вопрос 7. Укажите, какие законы РФ относятся к законам об информатизации и защите информации?

Выберите один или несколько ответов:

a. "О коммерческой тайне";

b. "О связи";

c. "Об участии в международном информационном обмене";

d. "О патентах".

Вопрос 8. Что относят к тайне частной жизни?

Выберите один или несколько ответов:

a. Тайна почтовых сообщений;

b. Тайна голосования;

c. Тайна исповеди;

d. Личная тайна.

Вопрос 9. Укажите, к какому типу конфиденциальной информации (КИ) относятся сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них?

Выберите один ответ:

a. личная КИ;

b. производственная КИ;

c. служебная КИ

d. судебно-следственная КИ;

e. профессиональная КИ;

f. коммерческая КИ.

Вопрос 10. Расставьте типы актов нормативной правовой базы по уровням.

1-й уровень - самый высокий

7-й уровень - самый низкий

a. Акты органов исполнительной власти;

b. Кодексы, Федеральные законы;

c. Нормативные документы уровня предприятий;

d. Постановления Правительства, Государственные стандарты;

e. Нормативные акты субъектов РФ;

f. Нормативные акты органов местного самоуправления;

g. Международные правовые акты;

Примерные оценочные материалы по Теме 3. Обеспечение кибербезопасности медиапроизводства

Доклад-презентация (контрольная работа):

Задание:

1. Выбрать тему (даны варианты примерных тем, но обучающийся вправе предложить свою тему, по его мнению более полезную для его будущей профессиональной деятельности) и зарегистрировать тему у своего преподавателя по дисциплине. План раскрытия темы (список наименований слайдов) обучающийся на учебном занятии или на онлайн-консультации обсуждает с преподавателем, ведущим дисциплину.
2. Необходимо материал подкрепить актуальными примерами и иллюстрациями (желательно скриншотами), составляющими практическую значимость (не менее 50%). Информация должна быть актуальна. Историю развития не освещать, а рассмотреть поставленные вопросы на современном этапе развития общества.
3. Разработать текст доклада. Оформить текст по требованиям вуза в документе Word. Пронумеровать текст в соответствии с нумерацией слайдов (см. п.4).
4. Разработать презентацию, иллюстрирующую информацию доклада (с иллюстрациями, схемами, списками и таблицами, определениями). Оформить презентацию в соответствии с требованиями, указанными в документе "Требования к оформлению презентаций".
5. В качестве ответа загрузить в Moodle файлы с текстом доклада и презентацией.
6. Доложить по теме на практическом занятии по дисциплине «Кибербезопасность», используя презентацию (не чтение текста, а выступление на основе материала реферата).
7. Ответить на вопросы слушателей.
8. Уяснить замечания преподавателя и при оценке "не зачтено" доработать и/или переработать материал (т.е. повторить п. 1-4 с учётом замечаний).

Критерии оценивания:

- новизна информации (информация об актуальных цифровых технологиях/инструментах/ресурсах с указанием конкретно кем и где на данный момент востребованы для обеспечения кибербезопасности; использовать источники информации не старше 5 лет; указать о новинках, которые будут в ближайшем будущем);
- доходчивость пояснения нового материала (введение терминологии из НПА и научной литературы; классификация; примеры, в том числе из судебной практики; представление сложно воспринимаемой информации в двух видах);
- актуальность информации (источники не старше 5 лет),
- освещение законодательства по вопросу (Российское законодательство на различных уровнях, законопроекты, международные акты, положительный опыт зарубежного правового регулирования вопроса, выявленные проблемы правового регулирования),
- рассмотрение вопроса о развитии и трендах (цели и задачи, польза, что будет в будущем, современные угрозы),
- примеры использования инструментария по обеспечению кибербезопасности (скриншоты, пошаговые инструкции, демоверсии, способы получения доступа к информации),
- практическая значимость (польза данной информации для применения в профессиональной и жизнедеятельности, методические рекомендации)...

ПРИМЕРНЫЕ темы доклада-презентации:

1. Информационная безопасность образовательного процесса. Актуальность включения дисциплины по информационной безопасности в программу среднего общего образования.
2. Политика информационной безопасности при работе в сети «Интернет»
3. Защита персональных данных
4. НПА области защиты информации. Правовые коллизии и дыры.
5. Положительный опыт зарубежных государств в правовом обеспечении информационной безопасности
6. Big Data: польза и угрозы
7. Польза и угрозы современных информационных технологий
8. Фиксация «электронных» доказательств. Юридическая сила электронной информации.
9. Возможные угрозы при цифровизации
10. Судебные компьютерные экспертизы. Применение ИТ для осуществления электронного уголовно-процессуального доказывания.
11. Специалисты в информационной безопасности
12. Социальная инженерия
13. Обеспечение ИБ при использовании беспроводных сетей
14. Статистика и примеры нарушений ИБ; «кибервойна»
15. Политика ИБ
16. Методика расследования преступлений в сфере компьютерных технологий.
17. Настройка безопасной работы ПК с ОС Windows
18. Восстановление потерянных данных
19. Электронная подпись
20. Защита сведений, относящихся в коммерческой тайне
21. Комплексная защита информации физического лица
22. Возможные угрозы информации физического лица
23. Противодействие мошенничеству
24. Стандарты и методики в области ИБ
25. Компании, основной функцией которых является защита информации (российские, в Алтайском крае, Новосибирской области)
26. Блокчейн и цифровые валюты: польза и угрозы
27. Теневой Интернет
28. Организационно-правовые вопросы информационной безопасности цифровой экономики
29. Цифровые права и цифровой след: польза и угрозы
30. Смарт-контракты и токены: польза и угрозы
31. Современные цифровые технологии: польза и угрозы
32. Массовые социально значимые услуги (сервисы), переведённые в электронный формат: польза и угрозы
33. Интернет вещей: польза и угрозы
34. Искусственный интеллект: польза и угрозы
35. Гаджеты, электронные устройства: польза и угрозы
36. Маркетплейсы: польза и угрозы
37. Виртуальная и дополненная реальность (VR и AR) : польза и угрозы
38. Облачные технологии: польза и угрозы
39. Мессенджеры: польза и угрозы

4.3. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код Компетенции	Наименование компетенции	Код компонента и(или) этапа компетенции	Наименование компонента и(или) этапа компетенции
ОПК-6	способен отбирать и внедрять в процесс медиапроизводства современные технические средства и информационно-коммуникационные технологии	ОПК-6.1	Способен оценивать потенциальные риски и угрозы безопасности при осуществлении продвижения социально значимых проектов
		ОПК-6.2	Способен отслеживать глобальные тенденции модернизации технических средств и информационно-коммуникационных технологий для осуществления профессиональной деятельности

Компонент компетенции	Индикатор оценивания	Критерий
ОПК-6.1	Способен оценивать потенциальные риски и угрозы безопасности при осуществлении продвижения социально значимых проектов	Владеет навыками оценки потенциальных рисков и угроз безопасности при осуществлении продвижения социально значимых проектов
ОПК-6.2	Способен отслеживать глобальные тенденции модернизации технических средств и информационно-коммуникационных технологий для осуществления профессиональной деятельности	Знает принципы создания современных медиатекстов с использованием современных технических средств и информационно-коммуникационных технологий для разных медийных платформ, владеет навыками безопасной работы в мультимедийных сервисах и приложениях

4.3.1. Типовые оценочные средства

Вопросы к зачёту:

1. Кибербезопасность как наука и научная дисциплина.
2. Актуальность защиты информации. Терминология области защиты данных.
3. Преступления в сфере компьютерной информации. Противоправные действия с информацией. Пути несанкционированного доступа к информации.
4. Система защиты информации. Проектирование системы обеспечения кибербезопасности.
5. Концептуальная модель кибербезопасности: угрозы информации, объекты угроз, цели злоумышленников, способы защиты информации, источники угроз, основные направления, средства защиты информации, действия, приводящие к неправомерному овладению конфиденциальной информацией.
6. Модели области защиты данных.

7. Направления обеспечения кибербезопасности: правовое, организационное и инженерно-техническое.

8. Комплексный подход к разработке системы защиты информации. Типовой порядок действий по обеспечению кибербезопасности.

9. Угрозы кибербезопасности профессиональной деятельности. Классификация угроз и специфические виды угроз для компьютерных сетей.

10. Цели, субъекты и уровни уязвимости кибербезопасности. Каналы утечки информации.

11. Предметные области кибербезопасности и ее субъекты.

12. Использование информации в компьютерных сетях для совершения правонарушений и преступлений.

13. Критерии безопасности компьютерных систем. Защита компьютерных систем.

14. Криптографическая защита. Электронная подпись.

15. Разграничение доступа, ролевое управление доступом. Идентификация и аутентификация.

16. Компьютерные вирусы и вредоносное программное обеспечение.

17. Восстановление данных. Анализ защищённости.

18. Служба защиты информации и её организационно-методическая работа. Мониторинг информационного обмена и аудит действий пользователей в компьютере.

19. Методы и средства физической, программной, аппаратной и криптографической защиты информации.

20. Правила поведения в сети «Интернет» и «компьютерная гигиена». Преступления в «киберпространстве», «кибервойна». Принципы кибербезопасности.

21. Экспертные группы, занимающиеся изучением инцидентов компьютерной безопасности.

22. Доступ к информации, классификация информации по доступу к ней.

23. Виды информации ограниченного доступа.

24. Обеспечение государственной тайны. Правовое регулирование государственной тайны.

25. Обеспечение коммерческой тайны. Правовое регулирование коммерческой тайны.

26. Структура и состав организационно-правового обеспечения коммерческой тайны. Проблемы правовой ответственности в сфере коммерческой тайны.

27. Обеспечение защиты персональных данных. Структура и состав организационно-правового обеспечения защиты персональных данных. Проблемы правовой ответственности в сфере персональных данных.

28. Виды служебной и профессиональной тайн. Правовое регулирование служебной и профессиональной тайны.

29. Объекты авторского и патентного права, их правовое регулирование.

30. Структура информационного законодательства о кибербезопасности в Российской Федерации.

31. Международное законодательства о кибербезопасности.

32. Правовое обеспечение безопасности в информационной сфере.

33. Государственные регуляторы в области информационной безопасности.

34. Защита прав граждан в информационной сфере.

35. Государственная политика в сфере обеспечения информационной безопасности.

36. Нормативные документы по кибербезопасности на уровне предприятия/организации.

37. Современные проблемы правового обеспечения кибербезопасности в России.

38. Положительный опыт зарубежных государств в правовом обеспечении кибербезопасности.

39. Интернет как явление и процесс. Нормативная правовая база по вопросам функционирования сети «Интернет» в России.

40. Правовые аспекты обеспечения безопасности в Интернете. Правовые проблемы Интернета.

Методические материалы

Оценочными средствами текущего контроля являются:

– тестовые задания;

– выполнение кейс-задания;

– подготовка доклада-презентации и выступление с ним на учебном занятии (контрольная работа);

– итоговый контроль – зачёт

Рейтинговая оценка по данной дисциплине в семестре складывается из текущих оценок посещаемости занятий, защиты результатов работ, выполняемых на практических занятиях, знаний на промежуточном контроле (тестирование по темам) и итоговой оценки на экзамене.

Изучение дисциплины предполагает использование различных форм усвоения учебного материала. На лекциях студенты должны уяснить сущность изучаемой темы курса, ее взаимосвязь с другими отраслями права.

На семинарских занятиях полученные на лекциях знания должны быть углублены на основе изучения теоретических вопросов темы во взаимосвязи с профессиональной деятельностью.

Кроме того, к основным видам учебных занятий относятся и практические занятия, которые направлены на подтверждение теоретических положений и формирование учебных и профессиональных практических умений.

Выполнение студентами практических занятий направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;

- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;

- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Наряду с формированием знаний, умений и навыков в процессе практических занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать теоретические знания на практике, развиваются интеллектуальные умения.

При решении практических задач студенты должны уметь решать поставленные задачи в соответствии с структурными возможностями информационных систем.

При решении практических задач студенты должны уметь решать поставленные задачи в соответствии с структурными возможностями информационных систем.

Оценивание обучающегося на зачёте по дисциплине

Знания, умения, действия обучающегося на экзамене оцениваются как «зачтено», «не зачтено».

Зачёт принимает преподаватель, ведущий практику с учетом результатов теоретического обучения на лекциях. Зачёт проводится в устной форме по билетам.

Преподавателю, принимающему зачёт предоставляется право задавать обучающимся дополнительные вопросы сверх билета, а также, помимо теоретических вопросов, давать ситуационные задачи и примеры, направленные на оценку умениевой и навыковой составляющих компетенций. При проведении зачёта используются технические средства.

Оценивание обучающегося на экзамене по дисциплине

Оценка зачёта (стандартная)	Требования к знаниям
«зачтено»	демонстрируются глубокие или частичные знания кибербезопасности, теоретических положений, на основе которых осуществляется защита информации в киберпространстве при реализации медиапроизводства, показываются хорошие умения практического использования информационных технологий защиты информации; выполнены и защищены значительная часть работ текущего контроля знаний
«незачтено»	фрагментарные знания кибербезопасности, теоретических положений, на основе которых осуществляется защита информации в киберпространстве при реализации медиапроизводства, не показываются умения практического использования информационных технологий защиты информации; отсутствует значительная часть работ текущего контроль знаний

5. Методические материалы по освоению дисциплины

Наряду с посещением семинаров и участием в обсуждении проблем, учебный план предусматривает затрату обучающимися, как правило, большего числа часов для самостоятельной работы.

5.1. Методические рекомендации по подготовке к практическим занятиям

Практическое занятие подразумевает решение типовых задач, разбор определенных ситуаций. Подготовка к практическому занятию начинается с тщательного ознакомления с условиями предстоящей работы, определившись с вариантом задачи, следует обратиться к рекомендуемой литературе. Задание должно быть охвачено полностью и рекомендованная литература должна быть освоена в большем объеме. Для полноценной подготовки к практическому занятию чтения учебников недостаточно, необходимо использовать Интернет-ресурсы. Тщательная подготовка к практическим занятиям, как и к лекциям, имеет определяющее значение: занятие пройдет так, как обучающийся подготовился к его проведению. Готовясь к практическим занятиям, следует активно пользоваться справочной литературой: энциклопедиями, словарями, и др. По окончании практического занятия к нему следует обратиться еще раз, повторив основные моменты – для этого в течение занятия следует делать пометки об используемых информационных технологиях.

5.2. Методические рекомендации по подготовке к выполнению типового задания (ТЗ)

Типовое задание является одной из основных форм текущего контроля преподавателем работы обучающегося.

Типовое задание представляет собой письменный ответ на вопрос, который рассматривается в рамках дисциплины.

Содержание ответа на поставленный вопрос включает:

– показ автором знания теории вопроса и понятийного аппарата,
– понимание механизма реально осуществляемой практики,
– выделение ключевых проблем исследуемого вопроса и их решение.

Структура (план) письменного ответа на типовое задание может иметь соответствующую рубрикацию.

Критерии оценки типового задания:

1. Знания и умения на уровне требований стандарта конкретной дисциплины: знание фактического материала, усвоение общих представлений, понятий, идей.
2. Характеристика реализации цели и задач исследования (новизна и актуальность поставленных в контрольной работе проблем, правильность формулирования цели, определения задач исследования, правильность выбора методов решения задач и реализации цели; соответствие выводов решаемым задачам, поставленной цели, убедительность выводов).
3. Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, логичность и последовательность изложения материала, корректность аргументации и системы доказательств, характер и достоверность примеров, иллюстративного материала, широта кругозора автора, наличие знаний интегрированного характера, способность к обобщению).
4. Качество полученных результатов (степень завершенности исследования, спорность или однозначность выводов).
5. Использование литературных источников.
6. Культура письменного изложения материала.
7. Культура оформления материалов работы.

Отчёт по выполнению кейс-задания должен быть оформлен в соответствии с требованиями Алтайского филиала РАНХиГС. Типовые задания оцениваются преподавателем дисциплины по шкале «незачтено/зачтено».

5.3. Подготовка к тестам контроля знаний (Т)

Подготовка к тестированию требует от обучающихся тщательного изучения материала по теме или блоку тем, где акцент делается на изучение причинно-следственных связей, раскрытию природы явлений и событий, проблемных вопросов. Для подготовки необходима рабочая программа дисциплины с примерами тестов, учебно-методическим и информационным обеспечением.

Оценивание тестовых заданий

Количество правильных ответов теста (%)	0-49	50-100
Зачтено/НЕ зачтено	НЕ зачтено	зачтено

5.4. Методические рекомендации по подготовке к зачёту

При подготовке к зачёту по дисциплине «Кибербезопасность» следует руководствоваться рабочей программой, что позволит четко представить круг вопросов, подлежащих изучению. При изучении дисциплины «Кибербезопасность» трудности в усвоении знаний могут возникнуть в связи с большим разнообразим информационных технологий и компьютерных средств. При этом каждое обеспечение информационной системы обладает собственным понятийным аппаратом. Соответственно, в рамках данной дисциплины обучающимся необходимо уяснить специфику программного, информационного, методического, правового, лингвистического и технического обеспечений автоматизированных информационных систем в государственном и муниципальном управлении. На настоящий момент имеется огромный массив документов по вопросам применения информационных технологий в государственном и муниципальном управлении. Для того чтобы сориентироваться в этом массиве обучающимся следует обратиться к перечню рекомендуемой литературы, сформированному для подготовки в рамках курса «Кибербезопасность». Еще одной «проблемой» при изучении данной дисциплины является быстрое изменения, происходящие в области информационных технологий. В связи с этим обучающимся следует учитывать, что по указанной причине в учебниках и учебных пособиях не всегда содержится актуальная

информация, касающаяся современных компьютерных средств. Поэтому в процессе самостоятельной работы обучающихся, при подготовке к зачёту необходимо уточнять актуальность подобранного материала. Необходимым условием успешного изучения данной дисциплины является свободное владение обучающимися понятиями области информационных и коммуникационных технологий. Приобретение глубоких знаний предполагает эффективное использование различных видов учебной работы: лекционных и практических занятий, самостоятельной работы.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет»

6.1. Основная литература

1. Белоус А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / Белоус А.И., Солодуха В.А.. — Москва, Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/98349.html.

2. Белоус А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / Белоус А.И., Солодуха В.А.. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/108023.html.

3. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : монография / О. А. Степанов. — Москва : Издательство Юрайт, 2020. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/448300.

4. Воронова, О. Е. Современные информационные войны: стратегии, типы, методы, приемы / О. Е. Воронова, А. С. Трушин. — Москва : Аспект Пресс, 2021. — 176 с. — ISBN 978-5-7567-1102-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/104482.html

5. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В.С. Овчинский. — Москва : Норма : ИНФРА-М, 2022. — 528 с. - ISBN 978-5-91768-814-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1837931

6.2. Дополнительная литература

1. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/103997.html

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450371.

3. Джонс, К. Д. Инструментальные средства обеспечения безопасности : учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102011.html

4. Проблемы создания цифровой экосистемы: правовые и экономические аспекты : монография / МГУ им. М.В. Ломоносова, Университет им. О.Е. Кутафина (МГЮА),

Моск. отделение Ассоциации юристов России, Межд. союз юристов и экономистов (Франция) ; Е. Н. Абрамова, А. П. Алексеенко, С. Н. Белова [и др.] ; под общ. ред. В. А. Вайпана,М. А. Егоровой. - Москва : Юстицинформ, 2021. - 276 с. - ISBN 978-5-7205-1728-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1481723.

5. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469866

6.4. Нормативные правовые документы и иная правовая информация

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями) информации". [Электронный ресурс]. URL: Гарант / Справочные правовые системы. 2018. Режим доступаwww.garant.ru.
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (с изменениями и дополнениями). [Электронный ресурс]. URL: Гарант / Справочные правовые системы. 2018. Режим доступа: www.garant.ru.
3. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы". Режим доступа: www.garant.ru.
4. "Паспорт национального проекта "Национальная программа "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) . Режим доступа: www.garant.ru.

6.5. Интернет-ресурсы

1. Официальный сайт ЗАО «КонсультантПлюс». Режим доступа: www.consultant.ru.
2. Официальный сайт ООО «НПП Гарант-Сервис». Режим доступа: www.garant.ru.
3. Портал правовой информации Российской Федерации. Режим доступа: pravo.gov.ru.
4. Центр реагирования на компьютерные инциденты. Режим доступа: https://www.cert.ru/ru/about.shtml.

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для обеспечения учебного процесса по дисциплине «Информационно-аналитические технологии государственного и муниципального управления» филиал располагает учебными аудиториями для проведения занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещениями для самостоятельной работы и помещениями для хранения и профилактического обслуживания учебного оборудования.

Лекционные аудитории оснащены видеопроекционным оборудованием для проведения презентаций, а также средствами звуковоспроизведения; помещения для практических занятий укомплектованы учебной мебелью; библиотека располагает рабочими местами с доступом к электронным библиотечным системам и сети интернет. Все учебные аудитории оснащены компьютерным оборудованием и лицензионным программным обеспечением.

Программное обеспечение:
Microsoft Windows 10 профессиональная
Microsoft Office ProPlus 2016
ESET NOD32 Antivirus Business Edition

система ГАРАНТ
Справочная правовая система КонсультантПлюс
Архиватор 7ZIP
Средство просмотра файлов PDF-формата Adobe Acrobat Reader
Браузер Google Chrome
Браузер Mozilla Firefox