

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

Институт общественных наук
Кафедра интегрированных коммуникаций

УТВЕРЖДЕНА

кафедрой интегрированных коммуникаций

Протокол от «25» ноября 2020 г. №3

РАБОЧАЯ ПРОГРАММА

Б1.В.ДВ.01.22.06 Безопасность в цифровой среде

(индекс, наименование дисциплины)

Minor "Маркетинговые коммуникации в цифровой среде»

38.03.02 Менеджмент

(код, наименование направления подготовки)

Стратегическое управление компанией (Liberal Arts)

направленность (профиль)

бакалавр

(квалификация)

очная

(форма обучения)

Год набора - 2021

Москва, 2020 г.

Автор–составитель:

Заведующий кафедрой интегрированных коммуникаций, к.э.н. М.В. Захарова

Заведующий кафедрой интегрированных коммуникаций, к.э.н. М.В. Захарова

Содержание

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы	4
2. Объем и место дисциплины в структуре ОП ВО.....	4
3. Содержание и структура дисциплины	5
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине	6
5. Методические указания для обучающихся по освоению дисциплины	12
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	15
6.1. Основная литература.	15
6.2. Дополнительная литература.	15
6.3. Учебно-методическое обеспечение самостоятельной работы.	16
6.4. Нормативные правовые документы.	16
6.5. Интернет-ресурсы.....	16
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы	16

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.ДВ.01.22.06 «Безопасность в цифровой среде» обеспечивает овладение следующими компетенциями с учетом индикатора:

Код компетенции	Наименование Компетенции	Код индикатора компетенции	Наименование индикатора компетенции
СК ОС LA-24	Способен анализировать данные в сети интернет для выбора оптимальных каналов коммуникации с потребителями в цифровой среде	СК ОС LA-24.1	Решает задачи, связанные с коммуникацией компании с потребителями в сети интернет, в сфере её маркетинговой деятельности, используя теоретические знания и практические навыки

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

Код индикатора компетенции	Результаты обучения
СК ОС LA-24.1	на уровне знаний: Основы законодательства Российской Федерации в области маркетинговой деятельности Основы методов и организационных возможностей управления изменениями Основы методов изучения внутреннего и внешнего рынка, его потенциала и тенденций развития цифровой среды
	на уровне умений: Участвовать в построении системы взаимодействия маркетинговой службы с другими подразделениями организации Участвовать в систематизации и обобщении больших объемов первичной и вторичной маркетинговой информации
	на уровне навыков: Участие в обеспечении контроля маркетинговой деятельности организации в цифровой среде Поиск первичной и вторичной маркетинговой информации в цифровой среде

2. Объем и место дисциплины в структуре ОП ВО

Дисциплина по учебному плану составляет 2 ЗЕ, т.е. 72 ак.ч./54 ас.ч, в том числе 28 ак.ч./21 ас.ч. – контактная работа с преподавателем виде практических занятий и 44 ак.ч./33 ас.ч. - самостоятельная работа обучающихся.

Б1.В.ДВ.01.22.06 «Безопасность в цифровой среде» входит в состав дисциплин minor по выбору вариативной части, изучается в 6 семестре вместе с дисциплиной Б1.В.ДВ.01.22.05 «Web-аналитика» и является основой для дисциплин Б1.В.ДВ.01.22.07

«Исследования в цифровой среде» и Б1.В.ДВ.01.22.08 «Анализ поведения интернет-пользователей».

3. Содержание и структура дисциплины

№ п/п	Наименование тем (разделов)	Объем, час.						Форма текущего контроля успеваемос ти*, промежудо чной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Информационная безопасность	12/9			4/3		8/6	Д, О
Тема 2	Антивирусная защита информации	14/10,5			6/4,5		8/6	ДО
Тема 3	Идентификация и проверка подлинности пользователя и электронная цифровая подпись	14/10,5			6/4,5		8/6	Д, О
Тема 4	Государственная политика в области обеспечения информационной безопасности	16/12			6/4,5		10/7,5	Д, О
Тема 5	Политика информационной безопасности предприятия	16/12			6/4,5		10/7,5	ДО
Промежуточная аттестация								Зачет с оценкой
Всего:		72/54			28/21		44/33	

Примечание: * - опрос (О), доклад (ДО), диспут (Д).

Содержание дисциплины

Тема 1. Информационная безопасность

Понятие информационной безопасности. Основные принципы информационной безопасности: целостность, конфиденциальность, доступность. Методы защиты информации в информационной системе.

Угрозы информационной безопасности: классификации, источники возникновения и пути реализации. Санкционированный и несанкционированный доступ к данным. Виды несанкционированного доступа к информации. Средства и механизмы защиты от несанкционированного доступа.

Тема 2. Антивирусная защита информации

Понятие компьютерного вируса, сущность и возможности проявления. Классификации компьютерных вирусов. Структура современных вирусных программ. Основные методы и средства защиты от воздействия компьютерных вирусов.

Современные пакеты антивирусных программ. Характеристики и возможности применения.

Тема 3. Идентификация и проверка подлинности пользователя и электронная цифровая подпись

Идентификация и аутентификация пользователя. Типовые схемы идентификации и аутентификации пользователя. Особенности применения пароля для аутентификации пользователя. Биометрическая идентификация и аутентификация. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний: упрощённая схема идентификации, параллельная схема идентификации.

Проблемы аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Алгоритмы электронной цифровой подписи. Алгоритм электронной цифровой подписи RSA. Отечественный стандарт хэш-функции. Отечественный стандарт цифровой подписи.

Тема 4. Государственная политика в области обеспечения информационной безопасности

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании Интернет. Интернет-мошенничество. Ответственность за преступления в сети Интернет. Правовые акты в области информационных технологий и защиты киберпространства. Защита персональных данных.

Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью.

Тема 5. Политика информационной безопасности предприятия

Разработка политики, основные этапы: классификация информации, формирование списка угроз, меры предотвращения и противодействия. Политика информационной безопасности для персонала. Компоненты архитектуры безопасности. Примеры политик безопасности крупных российских и международных компаний. Стандарты безопасности.

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

4.1. Формы и методы текущего контроля успеваемости, обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.ДВ.01.22.06 «Безопасность в цифровой среде» используются следующие методы текущего контроля успеваемости обучающихся:

при проведении занятий семинарского типа: опрос, диспут;

при контроле результатов самостоятельной работы студентов: доклад.

4.1.2. Форма и средства (методы) проведения промежуточной аттестации

Промежуточная аттестация проводится в виде зачёта с оценкой в форме устного ответа на два вопроса из предложенного списка.

4.2. Материалы текущего контроля успеваемости

Глубокое усвоение материала обеспечивается сочетанием практических занятий и самостоятельной работы студентов с литературой, работой в групповых проектах.

Вопросы для самостоятельной подготовки по темам.

Тема 1. Информационная безопасность

1. Понятие информационной безопасности.
2. Основные принципы информационной безопасности: целостность, конфиденциальность, доступность.
3. Методы защиты информации в информационной системе.
4. Угрозы информационной безопасности: классификации, источники возникновения и пути реализации.
5. Санкционированный и несанкционированный доступ к данным.
6. Виды несанкционированного доступа к информации.
7. Средства и механизмы защиты от несанкционированного доступа.

Тема 2. Антивирусная защита информации

1. Понятие компьютерного вируса, сущность и возможности проявления.
2. Классификации компьютерных вирусов.
3. Структура современных вирусных программ.
4. Основные методы и средства защиты от воздействия компьютерных вирусов.
5. Современные пакеты антивирусных программ.

Тема 3. Идентификация и проверка подлинности пользователя и электронная цифровая подпись

1. Идентификация и аутентификация пользователя.
2. Типовые схемы идентификации и аутентификации пользователя.
3. Биометрическая идентификация и аутентификация.
4. Взаимная проверка подлинности пользователей.
5. Протоколы идентификации с нулевой передачей знаний: упрощённая схема идентификации, параллельная схема идентификации.
6. Проблемы аутентификации данных и электронная цифровая подпись.
7. Однонаправленные хэш-функции.
8. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
9. Алгоритмы электронной цифровой подписи.
10. Алгоритм электронной цифровой подписи RSA.
11. Отечественный стандарт хэш-функции.
12. Отечественный стандарт цифровой подписи.

Тема 4. Государственная политика в области обеспечения информационной безопасности

1. Собственность в Интернете.
2. Авторское право.
3. Интеллектуальная собственность.
4. Платная и бесплатная информация.
5. Защита прав потребителей при использовании Интернет.
6. Интернет-мошенничество.
7. Ответственность за преступления в сети Интернет.
8. Правовые акты в области информационных технологий и защиты киберпространства.
9. Защита персональных данных.

10. Зарубежные стандарты и международные соглашения в области информационной безопасности.
11. Международное сотрудничество в области борьбы с компьютерной преступностью.

Тема 5. Политика информационной безопасности предприятия

1. Разработка политики информационной безопасности, основные этапы.
2. Политика информационной безопасности для персонала.
3. Компоненты архитектуры безопасности.
4. Стандарты безопасности.

Примерная тематика диспутов

1. Кибербезопасность как фактор оценки развития цифровой экономики.
2. Техника безопасности при регистрации на веб-сайтах.
3. Компьютерное пиратство.
4. Плагиат.
5. Оценка ущерба от киберпреступлений.
6. Ответственность за киберпреступления.
7. Коммерческое, бесплатное и лицензионное ПО.
8. Виды лицензий на ПО.
9. Информационные войны.
10. Информационное окружение.
11. Защита киберпространства как одна из задач государства.
12. Военная, государственная и коммерческая тайна.
13. Защита сайтов коммерческих организаций.
14. Защита сайтов государственных организаций.

Примерные темы докладов

1. Стратегия обеспечения информационной безопасности предприятия.
2. Информационная безопасность в бизнесе.
3. Сертификация, лицензирование, сертификация и аттестация в области информационной безопасности.
4. Служебная тайна.
5. Коммерческая тайна.
6. Государственная тайна.
7. Экономика и правовые основы рынка интеллектуальной собственности.
8. Экономическая информационная безопасность.
9. Закон РФ об электронной цифровой подписи.
10. Управление криптографическими ключами: генерация, хранение, распределение ключей.
11. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. No Пр-1895).
12. Закон РФ от 5 мая 1992 года No 2446-1 «О безопасности».
13. Закон РФ от 27 июля 2006 года No 149-ФЗ «Об информации, информационных технологиях и о защите информации».
14. Безопасность платёжных систем.
15. Безопасность систем бронирования билетов.
16. Безопасность при удалённом доступе к ресурсам компьютера.

17. Хакерские атаки.
18. Виды хакерских атак.
19. Угрозы для мобильных устройств.
20. Кибершпионаж.

4.3. Промежуточная аттестация

4.3.1. Перечень компетенций образовательной программы. Индикаторы и критерии оценивания компетенций

Код компетенции	Наименование компетенции	Код индикатора компетенции	Наименование индикатора компетенций
СК ОС LA-24	Способен анализировать данные в сети интернет для выбора оптимальных каналов коммуникации с потребителями в цифровой среде	СК ОС LA-24.1	Решает задачи, связанные с коммуникацией компании с потребителями в сети интернет, в сфере её маркетинговой деятельности, используя теоретические знания и практические навыки

Индикатор оценивания	Критерии Оценивания
СК ОС LA-24.1 Решает задачи, связанные с коммуникацией компании с потребителями в сети интернет, в сфере её маркетинговой деятельности, используя теоретические знания и практические навыки	<p>Базовый уровень - знает основные инструменты маркетинговых коммуникаций в сети интернет и тенденции их развития</p> <p>Повышенный уровень – может анализировать информацию, полученную из самостоятельно подобранных интернет-источников, для выявления преимуществ и недостатков различных коммуникационных инструментов сети интернет, используемых компаниями в маркетинговой деятельности.</p>

4.3.2. Типовые оценочные средства

Зачёт с оценкой в форме устного ответа на два вопроса из предложенного списка.

Примерные вопросы зачёта с оценкой:

1. Понятие информационной безопасности.
2. Основные принципы информационной безопасности: целостность, конфиденциальность, доступность.
3. Методы защиты информации в информационной системе.
4. Угрозы информационной безопасности: классификации, источники возникновения и пути реализации.
5. Санкционированный и несанкционированный доступ к данным.
6. Виды несанкционированного доступа к информации.
7. Средства и механизмы защиты от несанкционированного доступа.
8. Понятие компьютерного вируса, сущность и возможности проявления.

9. Классификации компьютерных вирусов.
10. Структура современных вирусных программ.
11. Основные методы и средства защиты от воздействия компьютерных вирусов.
12. Современные пакеты антивирусных программ.
13. Идентификация и аутентификация пользователя.
14. Типовые схемы идентификации и аутентификации пользователя.
15. Биометрическая идентификация и аутентификация.
16. Взаимная проверка подлинности пользователей.
17. Протоколы идентификации с нулевой передачей знаний: упрощённая схема идентификации, параллельная схема идентификации.
18. Проблемы аутентификации данных и электронная цифровая подпись.
19. Однонаправленные хэш-функции.
20. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
21. Алгоритмы электронной цифровой подписи.
22. Алгоритм электронной цифровой подписи RSA.
23. Отечественный стандарт хэш-функции.
24. Отечественный стандарт цифровой подписи.
25. Собственность в Интернете.
26. Авторское право.
27. Интеллектуальная собственность.
28. Платная и бесплатная информация.
29. Защита прав потребителей при использовании Интернет.
30. Интернет-мошенничество.
31. Ответственность за преступления в сети Интернет.
32. Правовые акты в области информационных технологий и защиты киберпространства.
33. Защита персональных данных.
34. Зарубежные стандарты и международные соглашения в области информационной безопасности.
35. Международное сотрудничество в области борьбы с компьютерной преступностью.
36. Разработка политики информационной безопасности, основные этапы.
37. Политика информационной безопасности для персонала.
38. Компоненты архитектуры безопасности.
39. Стандарты безопасности.

Шкала оценивания.

Форма промежуточной аттестации	Критерии оценивания	Оценка (баллы)
Устный ответ на зачете с оценкой	1. Полно раскрыто содержание материала билета: исчерпывающие и аргументированные ответы на вопросы в билете. 2. Материал изложен грамотно, в определенной логической	(31-40)

Форма промежуточной аттестации	Критерии оценивания	Оценка (баллы)
	<p>последовательности, не требует дополнительных пояснений, точно используется терминология.</p> <p>3. Демонстрируются глубокие знания дисциплин специальности.</p> <p>4. Даны обоснованные ответы на дополнительные вопросы</p>	
	<p>1. Ответы на поставленные вопросы в билете излагаются систематизировано и последовательно.</p> <p>2. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер, в изложении допущены небольшие пробелы (неточности), не исказившие содержание ответа.</p> <p>3. Материал излагается уверенно, в основном правильно даны все определения и понятия.</p> <p>4. При ответе на дополнительные вопросы комиссии полные ответы даны только при помощи наводящих вопросов.</p>	(21-30)
	<p>1. Неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса.</p> <p>2. Имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после наводящих вопросов.</p> <p>3. Демонстрируются поверхностные знания дисциплин специальности; имеются затруднения с выводами.</p> <p>4. При ответе на дополнительные вопросы комиссии ответы даются только при помощи наводящих вопросов.</p>	(11-20)
	<p>1. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине, не раскрыто его основное содержание.</p> <p>2. Допущены грубые ошибки в определениях и понятиях, при использовании терминологии, которые не исправлены после наводящих вопросов.</p> <p>3. Демонстрирует незнание и непонимание существа экзаменационных вопросов.</p> <p>4. Не даны ответы на дополнительные или наводящие вопросы комиссии.</p>	(0-10)

В течение семестра	Промежуточная аттестация	ИТОГО
0-60 баллов	Max 0-40 баллов	Max 100 баллов

В течение семестра обучающие выполняют практическое задание, готовят доклад по выбранной теме, участвуют в диспутах и обсуждениях. Общая сумма баллов за работу в семестре 60.

Промежуточная аттестация проходит в виде устного зачёта, за который можно набрать 40 баллов.

Шкала итоговых баллов за курс

<i>Сумма баллов за дисциплину</i>	<i>Зачет</i>	<i>Зачет с оценкой</i>	<i>Экзамен</i>
0 – 40	Не зачтено	Не зачтено (неудовлетворительно)	Неудовлетворительно
41 – 60	Зачтено	Зачтено (удовлетворительно)	Удовлетворительно
61 – 80	Зачтено	Зачтено (хорошо)	Хорошо
81- 100	Зачтено	Зачтено (отлично)	Отлично

4.4. Методические материалы

В процессе преподавания данной дисциплины используются как классические методы обучения (семинары), так и различные виды самостоятельной работы студентов по заданию преподавателя, которые направлены на развитие творческих качеств студентов и на поощрение их интеллектуальных инициатив.

В рамках данного курса используются такие активные формы обучения, как: подготовка докладов.

В процессе преподавания выполняется общеобразовательная задача: совершенствуется навык применения критического анализа при работе с информацией, расширяется культурный и профессиональный кругозор студентов. Одновременно выполняется и воспитательная задача – формирование активной жизненной позиции студентов, воспитание толерантности и уважения к духовным ценностям разных стран и народов. Студенты приобретают навыки и умения не только самостоятельной, но и совместной работы в группах, что способствует формированию умения общения друг с другом в коллективе, быть полноправным членом рабочей группы общества.

Данная программа строится с учётом ряда педагогических и методических принципов.

Принцип культурной и педагогической целесообразности основывается на отборе тематики курса.

Принцип автономии студентов реализуется открытостью информации для студентов о структуре курса, требованиях к выполнению заданий, содержание контроля и критериях оценивания разных видов устной и письменной работы. Организация аудиторной и самостоятельной работы обеспечивает определённый уровень личной ответственности студента за результаты.

5. Методические указания для обучающихся по освоению дисциплины

Дисциплина Б1.В.ДВ.01.22.06 «Безопасность в цифровой среде» изучается на протяжении одного семестра и завершается зачётом с оценкой. В ходе обучения основными видами учебных занятий являются семинарские занятия. В ходе семинарских занятий рассматриваются основные понятия тем, углубляются и закрепляются знания студентов по ряду рассмотренных вопросов, развиваются навыки в соответствии с этапами формирования компетенций.

<p align="center">Организация деятельности студента по видам учебных занятий</p>

Вид учебных занятий	Организация деятельности студента
Практические занятия	<p>На практических занятиях осуществляется проработка содержания курса. При подготовке к практическим занятиям студентам необходимо ознакомиться с источниками, учебной литературой, рекомендуется конспектировать источники.</p> <p>Во время практических занятий возможна такая форма работы как устные выступления студентов по контрольным вопросам семинарского занятия. Выступление на семинаре должно быть компактным и вразумительным, без неоправданных отступлений и рассуждений. Выступление предполагает самостоятельное изложение материала, вдумчивое и свободное. Важно помнить, что, выступая на занятии, студент обращается к группе, а не только к преподавателю. В свою очередь, остальные студенты должны осознавать важность вовлеченного участия в занятии, слушать, задавать вопросы выступающему, формулировать ответные реплики. По окончании занятия студенту рекомендуется повторить выводы, сконструированные на семинаре, проследив логику их построения, отметив положения, лежащие в их основе. Для облегчения реализации этой задачи во время занятия рекомендуется делать пометки. В случае неточностей и (или) непонимания какого-либо вопроса пройденного материала студенту следует обратиться к преподавателю для получения необходимой консультации и разъяснения возникшей ситуации.</p>
Доклад	<p>Тема доклада (реферата) выбирается студентом по согласованию с преподавателем. Важно при этом учитывать ее актуальность, научную разработанность, возможность нахождения необходимых источников для изучения темы реферата (доклада), имеющиеся у студента начальные знания и личный интерес к выбору данной темы.</p> <p>После выбора темы реферата (доклада) составляется перечень источников (монографий, научных статей, справочной литературы, содержащей комментарии, результаты исследований и т.п.).</p> <p>Реферат (доклад) - это самостоятельная учебно-исследовательская работа студента, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер.</p> <p>Примерные этапы работы над рефератом (докладом):</p> <ul style="list-style-type: none"> - формулирование темы; - подбор и изучение основных источников по теме (как правило, не менее 10); - составление библиографии; - обработка и систематизация информации; - разработка плана; - написание реферата (доклада); - публичное выступление с результатами исследования.
Групповая дискуссия, диспут	Групповая дискуссия - это средство, которое позволяет определить уровень сформированности профессиональных

	<p>навыков в условиях максимально приближенных к профессиональной среде. Модерацией дискуссии занимается преподаватель, который предлагает актуальную тему для дискуссии, ставит вопросы, акцентирует внимание аудитории на наиболее значимых аспектах.</p> <p>Проведение групповой дискуссии позволяет оценить формирование у студента соответствующих навыков, в том числе умение ставить проблему, обосновывать пути ее возможного разрешения, умение вести цивилизованный диалог, отстаивать свою точку зрения, аргументировано отвечать на правовые позиции иных участников групповой дискуссии, способность «на ходу» оценивать свои и чужие аргументы и факты, свободно оперировать фактическим материалом и без предварительной подготовки обрабатывать возникающие вопросы и проблемы.</p> <p>Семинар-дискуссия может содержать элементы «мозгового штурма»: участники стремятся выдвинуть как можно больше идей, не подвергая их критике; потом выделяются главные, они обсуждаются и развиваются, оцениваются возможности их доказательства или опровержения.</p>
--	--

Подготовка индивидуальных докладов и выполнение презентаций по темам курса

Критерии оценивания доклада и презентации:

Доклад – один из видов монологической речи, публичное развёрнутое официальное сообщение по определённому вопросу, основанное на привлечении документальных данных. Может быть устным или письменным. **В учебных целях:** доклад – вид самостоятельной научно-исследовательской работы, где автор раскрывает суть исследуемой проблемы; приводит различные точки зрения, а также собственные взгляды на нее.

Этапы работы над докладом. Подбор и изучение основных источников по теме (как и при написании реферата рекомендуется использовать не менее 8 - 10 источников). Составление библиографии. Обработка и систематизация материала. Подготовка выводов и обобщений. Разработка плана доклада. Написание. Публичное выступление с результатами исследования. В докладе соединяются три качества исследователя: умение провести исследование, умение преподнести результаты слушателям и квалифицированно ответить на вопросы.

Отличительными чертами доклада является научный, академический стиль изложения, логичность, последовательность, ясность, точность, аргументированность.

Доклад предполагает чёткое определение темы, связанной с научной проблемой. Преподаватель оценивает, насколько подготовленное студентом выступление отвечает заявленной им теме. Текст доклада должен иметь стройную композицию, должен быть хорошо структурирован, для чего студент должен уметь строить выступление по заранее определённому плану. Оценивается свободное владение текстом, умение строить устное высказывание, а не зачитывать текст по листу. Допускается только чтение цитат из научных источников или примеров. Студент должен выделить в своём выступлении основные положения, которые надо сформулировать в виде тезисов и продиктовать коллегам. Отдельно оценивается не только содержание доклада, но и форма его подачи: умение устанавливать контакт с аудиторией, умение улавливать реакцию слушателей, получать обратную связь, отвечать на возникающие вопросы. Доклад предполагает жёсткий хронометраж (по предварительной договорённости с преподавателем - до 10 минут). Необходимо обязательно уложиться в установленное время, успев сделать вывод (заключение). Материал может требовать дополнительных иллюстраций: схем, таблиц,

небольших рисунков, которые можно разместить в презентации.

Презентация позволяет иллюстрировать основные положения доклада и делать приведённые в выступлении примеры наглядными. Она не должна полностью воспроизводить текст выступления. По правилам, информация, приведённая устно, не должна полностью копироваться на слайдах.

Выделяют множество разнообразных видов презентаций. Основными являются: конспект выступления; таблица; схемы и графики; тестирование; слайд-шоу; модульный доклад; и т.п.

Иллюстративный материал должен быть достаточным, но не чрезмерным, и не иметь развлекательный, игровой характер. Анимированный рисунок в качестве украшения отвлекает внимание

Практические рекомендации при подготовке презентации:

1. Используйте не более двух типов шрифтов.
2. Оптимальное количество строк не более семи.
3. Количество символов в строке не более сорока (в том числе пробелы).
4. Использование заглавных и строчных букв облегчает чтение и распознавание слов. Использование цвета, больших букв, усиление жирности, курсивный шрифт помогают выделить главное.

5. Лучше читается шрифт без засечек (например, Arial). Оптимальные шрифты (заголовок – 24-32; подзаголовок – 2-24; основной текст – 18-24; подписи данных – 20-2)

6. Старайтесь использовать простые, короткие предложения: чем лаконичнее текст, тем выше концентрация внимания на ключевых словах).

Презентация не должна требовать подключения к Internet и выполнять сторонние приложения (например, анимационные ролики, которые требуют установки кодеков и др.).

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Семенов, Ю.А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс]: учебное пособие/ Семенов Ю.А.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 581 с.— Режим доступа: <http://www.iprbookshop.ru/94863.html>.— ЭБС «IPRbooks»

2. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Галатенко В.А.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 266 с.— Режим доступа: <http://www.iprbookshop.ru/97562.html>.— ЭБС «IPRbooks»

6.2. Дополнительная литература.

1. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет [Электронный ресурс]/ (Гутникова)А.С. Дупан [и др.].— Электрон. текстовые данные.— Москва: Издательский дом Высшей школы экономики, 2018.— 341 с.— Режим доступа: <http://www.iprbookshop.ru/89373.html>.— ЭБС «IPRbooks»

2. Петренко, С.А. Политики безопасности компании при работе в Интернет [Электронный ресурс]/ Петренко С.А., Курбатов В.А.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 397 с.— Режим доступа: <http://www.iprbookshop.ru/63807.html>.— ЭБС «IPRbooks»

6.3. Учебно-методическое обеспечение самостоятельной работы.

Положение об организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. приказа РАНХиГС от 11.05.2016 г. № 01-2211).
http://www.ranepa.ru/images/docs/prikazy-ranhigs/Pologenie_o_samostoyatelnoi_rabote.pdf

6.4. Нормативные правовые документы.

1. Федеральный закон от 13.03.2006 N 38-ФЗ (ред. от 08.03.2015) "О рекламе" (с изм. и доп., вступ. в силу с 25.05.2015)
2. Закон РФ «О средствах массовой информации» от 27 декабря 1991 г. (с последующими изменениями).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. No Пр-1895).
4. Закон РФ от 5 мая 1992 года No 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года No 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6.5. Интернет-ресурсы.

1. www.marketing.spb.ru – Энциклопедия маркетинга. Один из наиболее популярных сайтов, посвященных маркетингу. Содержит информацию как теоретического (публикации по маркетингу, библиография), так и практического (перечень маркетинговых фирм, отчеты по исследованиям) характера.
2. <http://www.4p.ru> – «4p.ru – е-журнал по маркетингу» – Сайт полностью посвящен маркетингу; содержит интересные теоретические материалы по различным аспектам маркетинга, а также раздел, посвященный результатам маркетинговых исследований. Кроме того, на сайте есть книжный магазин деловой литературы, каталог ссылок на ресурсы сети.
3. <http://www.e-xecutive.ru/> - сообщество эффективных менеджеров
4. <http://www.advi.ru> - рекламные идеи
5. <http://www.advertology.ru/> - наука о рекламе: электронный ресурс

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

Требования к аудиториям (помещениям) для проведения занятий:

Для проведения практических занятий по дисциплине необходимо наличие ноутбука (компьютера) с установленным пакетом Microsoft® и мультимедийного проектора.

Требования к программному обеспечению общего пользования:

Специализированное оборудование и специализированное программное обеспечение при изучении дисциплины не используется.