

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА
(МГЮА)»**

Кафедра информационного права и цифровых технологий

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Цифровой этикет и безопасность в сети Интернет**

ОП.20

год набора 2023

Код и наименование специальности:	40.02.01 Право и организация социального обеспечения
Уровень образования, на базе которого осуществляется подготовка специалистов:	основное общее
Форма (формы) обучения:	очная
Квалификация:	юрист

Москва - 2023

Программа утверждена на заседании кафедры информационного права и цифровых технологий, протокол № 9 от «10» мая 2023 года.

Автор:

Дженакова Екатерина Всеволодовна – преподаватель кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА)

Рецензент:

Дженакова Е.В. Цифровой этикет и безопасность в сети Интернет: рабочая программа дисциплины / Е.В. Дженакова. — М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2023.

Программа составлена в соответствии с требованиями ФГОС СПО.

©Университет имени О.Е. Кутафина (МГЮА), 2023.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (ПАСПОРТ).....	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	4
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	10
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ.....	11

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (ПАСПОРТ) «Цифровой этикет и безопасность в сети Интернет»

1.1. Место дисциплины в структуре основной образовательной программы:

Дисциплина «Цифровой этикет и безопасность в сети Интернет» является обязательной частью профессионального учебного цикла образовательной программы среднего профессионального образования в соответствии с ФГОС СПО по специальности 40.02.01. Право и организация социального обеспечения

Особое значение дисциплина имеет при формировании и развитии ОК1, ОК 4, ОК 5, ОК 6, ОК 11, ПК 1.2, ПК 1.6, ПК 2.3

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК1, ОК 4, ОК 5, ОК 6, ОК 11 ПК 1.2 ПК 1.6 ПК 2.3.	<ul style="list-style-type: none"> - осуществлять социальное взаимодействие, вести деловую переписку; - осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач; - использовать информационно-коммуникационные технологии в профессиональной деятельности 	<ul style="list-style-type: none"> - общепринятые правила общения, поведения. Деловой этикет, принципы делового общения; - понятие информационной культуры. Основы цифровой гигиены. Способы распознавания недостоверной информации; - основы информационной безопасности (социальный и правовой аспекты); - информационные риски и угрозы, методы противодействия.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Очная форма обучения

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	54
в том числе в форме практической подготовки	24
в т. ч.:	
Лекции	12

Практические занятия	12
Семинарские занятия	12
Консультации	2
<i>Самостоятельная работа</i>	16
Промежуточная аттестация	дифференцированный зачет

2.2. Тематический план и содержание учебной дисциплины

Очная форма обучения

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем, акад. ч. / в том числе в форме практической подготовки, акад. ч.	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Мораль и этика		12	ОК1, ОК 4, ОК 5, ОК 6, ОК 11 ПК 1.2 ПК 1.6 ПК 2.3
Тема 1. Мораль, этика, этикет	Содержание учебного материала	4	
	Лекция № 1 Понятие морали, этики, этикета. История формирования. Соотношение этики и морали.	2	
	Семинарское занятие № 1 Соотношение понятий: «этика», «мораль», «нравственность», «духовность». Культура, этика, этикет. Этические принципы и нормы в деловых отношениях	2	
	Самостоятельная работа обучающихся: Основные принципы гуманизма. Гарантии основных прав человека (права на свободу, на доступ к информации, на гласность, на свободу слова, презумпция невиновности, равный доступ к общественным благам). Деловая переписка: правила, принципы	4	
Тема 2. Деловой этикет.	Содержание учебного материала	4	
	Лекция № 2 Понятие делового этикета. Принципы делового этикета. Деловая переписка: правила, принципы	2	

	Практическое занятие № 1 Деловое письмо	2	
Раздел 2. Цифровой этикет		10	
Тема 3. Цифровой этикет: понятие, правила поведения в сети	Содержание учебного материала	4	ОК1 ОК 4 ОК 5 ОК 6 ОК 11 ПК 1.2 ПК 1.6 ПК 2.3
	Лекция № 3 Цифровой этикет Поведение в социальных сетях.	2	
	Семинарское занятие № 3 Понятие сетевого (цифрового) профиля. Формирование сетевого (цифрового) профиля. Цифровой след	2	
	Самостоятельная работа Цифровой след: понятие, формирование. Цифровая гигиена. Понятие «Digital detox»	6	
Раздел 3. Информационная и цифровая гигиена. Недостоверная информация, фейки		16	
Тема 4. Информационная и цифровая гигиена.	Содержание учебного материала	4	ОК1 ОК 4 ОК 5 ОК 6 ОК 11
	Лекция № 4 Понятие информационной и цифровой гигиены, их соотношение	2	
	Практическое занятие № 2 Понятие «Digital detox»: необходимость или ответ времени.	2	
Тема 5. Недостоверная информация, фейки	Содержание учебного материала	6	ПК 1.2 ПК 1.6 ПК 2.3
	Семинарское занятие № 4 Понятие «фейк», «недостоверная информация», «дезинформация», «ложная информация»: сходства и отличия	2	
	Практическое занятие № 3 Фейки, виды фейков, приемы распознавания фейков.	2	
	Практическое занятие № 4 Слухи, домыслы, сплетни. Достоверность информации в сети «Интернет». Создание фейков	2	
	Самостоятельная работа: 1. Понятие риска. Информационные риски и риски информационной	6	

	безопасности. 2. Рисксовая ситуация: понятие, характерные признаки. 3. Методики оценки информационных рисков: качественные и количественные (российские и зарубежные).		
Раздел 4. Информационная культура		4	
Тема 6. Информационная культура	Содержание учебного материала	4	ОК1, ОК 4, ОК 5, ОК 6, ОК 11 ПК 1.2 ПК 1.6 ПК 2.3
	Семинарское занятие № 5 Информационная культура	2	
	Практическое занятие № 5 Понятия «культура», «информационная культура», «компьютерная грамотность», «информационная грамотность», их соотношение	2	
Раздел 5. Информационная безопасность		16	
Тема 7. Информационная безопасность	Содержание учебного материала	6	ОК1 ОК 4 ОК 5 ОК 6 ОК 11 ПК 1.2 ПК 1.6 ПК 2.3
	Лекция № 5 Информационная безопасность: основные понятия, документы.	2	
	Семинарское занятие № 5 Информационные риски. Понятия «идентификация рисков» «оценка рисков», «управление рисками». Методики оценки рисков информационной безопасности	2	
	Практическое занятие № 6 Угрозы информационной безопасности, источники угроз	2	
	Самостоятельная работа Составьте таблицу информационных угроз обществу и государству Кибертравля: понятие, группы риска, противодействие (социальный и правовой аспект).	6	

Тема 8. Информационная безопасность личности	Содержание учебного материала	4	
	Лекция № 6 Угрозы личности в информационной среде	2	
	Семинарское занятие № 6 Информационные угрозы и источники угроз личности, способы защиты	2	
Консультации		2	
Промежуточная аттестация в форме		дифференцированного зачета	
Всего:		54	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Программно-аппаратное обеспечение реализации программы

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения, оснащенные оборудованием, а также соответствующее программное обеспечение.

Кабинеты «Профессиональных дисциплин», оснащенный оборудованием: рабочее место для преподавателя, компьютер, рабочие места для студентов, моноблок (микрофон, камера), проектор, магнитно-маркерная доска, беспроводная сеть Wi-fi.

Компьютерные классы, оснащенные: основным программным обеспечением, а также пакетом прикладных программ общего назначения (включающим текстовый процессор, графический редактор), доступом в сеть «Интернет».

3.2. Информационное обеспечение реализации программы

3.2.1. Основная литература:

1. Минбалеев, А. В. Проблемы цифрового права : Учебное пособие / А. В. Минбалеев. – Саратов : Амирит, 2022. – 234 с. – ISBN 978-5-00207-136-4. – URL: <https://www.elibrary.ru/item.asp?id=50304996> (дата обращения: 04.07.2023). – Режим доступа : [Инструкции по подключению и работе с электронными ресурсами](#). – Текст : электронный.

2. Фейковизация как средство информационной войны в интернет-медиа : научно-практическое пособие / Е. И. Галяшина, В. Д. Никишин, К. М. Богатырев и др. — Москва : Блок-Принт, 2023. — 144 с. - ISBN 978-5-604-86225-4. - URL: <http://ebs.prospekt.org/book/46733> (дата обращения: 04.07.2023). – Режим доступа : [Инструкции по подключению и работе с электронными ресурсами](#). – Текст : электронный.

3.2.2. Дополнительная литература

1. Мамина, Р. И. Сетевое общество и его реалии: цифровой этикет / Р. И. Мамина, Е. Е. Елькина – Текст : электронный. // Дискурс. – 2019. – Т. 5, № 2. – С. 24-34. (дата обращения: 04.07.2023). – Режим доступа : [Инструкции по подключению и работе с электронными ресурсами](#).

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 243 с. — ISBN 978-5-534-12774-4. — URL: <https://urait.ru/bcode/518441> (дата обращения: 04.07.2023). – Режим доступа : [Инструкции по подключению и работе с электронными ресурсами](#). – Текст : электронный.

3. Пэтчин Д. Написанное остается. Как сделать интернет-общение безопасным и комфортным / Д. Пэтчин, С. Хиндуя ; пер. с англ. В. Башкировой. – Москва : Манн, Иванов и Фербер, 2020. – 160 с. - URL: <https://www.litres.ru/book/justin-w-patchin/napisannoe-ostaetsya-kak-sdelat-internet-obschenie-bezopa-62735366/> (дата обращения: 04.07.2023). – Режим

доступа: по запросу [для зарегистрированных пользователей](#) (см. [инструкцию](#)). – Текст: электронный.

3.2.3. Нормативно-правовые акты и иные правовые документы:

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) [«Об информации, информационных технологиях и о защите информации»](#).
2. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.07.2021) [«О защите детей от информации, причиняющей вред их здоровью и развитию»](#).
3. Федеральный закон от 26.07.2017 № 187-ФЗ [«О безопасности критической информационной инфраструктуры Российской Федерации»](#)
4. Решение Конституционного Суда РФ от 13.02.2018 [«Об утверждении Обзора практики Конституционного Суда Российской Федерации за четвертый квартал 2017 года»](#).
5. Указ Президента РФ от 11.09.2012 № 1285 (ред. от 21.09.2017) [«О мерах по защите интересов Российской Федерации при осуществлении российскими юридическими лицами внешнеэкономической деятельности»](#).
6. Указ Президента РФ от 09.05.2017 № 203 [«О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»](#).
7. Указ Президента РФ от 05.12.2016 № 646 [«Об утверждении Доктрины информационной безопасности Российской Федерации»](#).
8. Указ Президента РФ от 28.06.1993 № 966 (ред. от 22.03.2005) [«О Концепции правовой информатизации России»](#).
9. Указ Президента РФ от 20.01.1994 № 170 (ред. от 09.07.1997) [«Об основах государственной политики в сфере информатизации»](#).

3.2.4. Интернет-ресурсы:

1. Справочно-правовая система Консультант Плюс: офиц.сайт. – URL: <http://www.consultant.ru> (дата обращения: 12.05.2023).
2. Видеоуроки в интернет. – URL: <http://www.videouroki.net/> (дата обращения: 12.05.2023).
3. Элементы большой науки: Популярный сайт о фундаментальной науке: офиц.сайт. – URL: <https://www.elementy.ru> (дата обращения: 12.05.2023).
4. Единая коллекция цифровых образовательных ресурсов. – URL: <http://www.school-collection.edu.ru> (дата обращения: 12.05.2023).
5. Мегаэнциклопедия Кирилла и Мефодия: офиц.сайт. – URL: <http://www.megabook.ru> (разделы «Наука /Математика. Кибернетика» и «Техника / Компьютеры и Интернет») (дата обращения: 12.05.2023).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Методы оценки</i>
В результате освоения учебной дисциплины обучающийся должен уметь:	Минимальный уровень не достигнут: обучающийся в результате	Текущая аттестация: <i>Письменный и</i>

<p>- осуществлять социальное взаимодействие, вести деловую переписку;</p> <p>- осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач;</p> <p>- использовать информационно-коммуникационные технологии профессиональной деятельности</p>	<p>набрал менее 50 % (баллов), продемонстрировав недостаточный уровень знаний и умений в рамках усвоенного учебного материала – неудовлетворительно.</p> <p>Минимальный уровень: обучающийся в результате набрал 50 - 69% (баллов), продемонстрировав удовлетворительный уровень знаний и умений в рамках усвоенного учебного материала – удовлетворительно.</p> <p>Средний уровень: обучающийся набрал 69 – 86% (баллов, продемонстрировав хорошие знания и умения в рамках усвоенного учебного материала – хорошо.</p> <p>Максимальный уровень: обучающийся набрал 86 – 100% (баллов), продемонстрировав отличные знания и умения в рамках усвоенного учебного материала – отлично*.</p>	<p>устный ответ на теоретические вопросы</p> <p>Промежуточная аттестация:</p> <p>дифференцированный зачет - контроль знаний</p>
<p>В результате освоения учебной дисциплины обучающийся должен знать:</p> <p>Общепринятые правила общения, поведения. Деловой этикет, принципы делового общения.</p> <p>Понятие информационной культуры. Основы цифровой гигиены. Способы распознавания недостоверной информации.</p> <p>Основы информационной безопасности (социальный и правовой аспекты). Информационные риски.</p>	<p>Минимальный уровень не достигнут: обучающийся в результате набрал менее 50 % (баллов), продемонстрировав недостаточный уровень знаний и умений в рамках усвоенного учебного материала – неудовлетворительно.</p> <p>Минимальный уровень: обучающийся в результате набрал 50 - 69% (баллов), продемонстрировав удовлетворительный</p>	<p>Текущая аттестация:</p> <p>Письменный и устный ответы на теоретические вопросы</p> <p>Промежуточная аттестация:</p> <p>дифференцированный зачет - контроль знаний</p>

	<p>уровень знаний и умений в рамках усвоенного учебного материала – удовлетворительно.</p> <p>Средний уровень: обучающийся набрал 69 – 86% (баллов, продемонстрировав хорошие знания и умения в рамках усвоенного учебного материала – хорошо.</p> <p>Максимальный уровень: обучающийся набрал 86 – 100% (баллов), продемонстрировав отличные знания и умения в рамках усвоенного учебного материала – отлично.</p>	
--	--	--