МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ У. Д. АЛИЕВА»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00991F81F759FC1D6837BA039630178332
Владелец: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КАРАЧАЕВО-ЧЕРКЕССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ У.Д. АЛИЕВА"
Действителен: с 19.06.2025 до 12.09.2026

УТВЕРЖДАЮ
Врио ректора
М.Х. Чанкаев
«25» // 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»

Карачаевск - 2025 г.

СОДЕРЖАНИЕ

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Дополнительная профессиональная образовательная программа повышения квалификации «Противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий» (далее - Программа), реализуемая Координационным центром по вопросам формирования у молодежи активной гражданской позиции, предупреждения межнациональных и межконфессиональных конфликтов, противодействия идеологии терроризма и профилактики экстремизма ФГБОУ ВО «Карачаево-Черкесский государственный университет имени У.Д. Алиева».

1.1 Нормативные правовые основания разработки программы

Программа разработана на основании:

– Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Федерального закона от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации»;

– Федерального закона «О федеральной службе безопасности» от 03.04.1995 № 40-ФЗ;

– Федерального закона от 30.11.2011 № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»;

– Профессионального стандарта «Следователь-криминалист» (утв. Приказом Минтруда и социальной защиты РФ от 23 марта 2015 г. № 183н);

– Приказа Министерства науки и высшего образования РФ от 31 августа 2020 г. № 1138 (в ред. от 27.02.2023) «Об утверждении федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.01 «Правовое обеспечение национальной безопасности»;

– Приказа Министерства науки и высшего образования РФ от 25 ноября 2020 г. № 1451 «Об утверждении федерального государственного образовательного стандарта высшего образования «Магистратратура по направлению подготовки 40.04.01 Юриспруденция»;

– Приказа Министерства науки и высшего образования РФ от 31 августа 2020 г. № 1136 (в ред. от 27.02.2023) «Об утверждении федерального государственного образовательного стандарта высшего образования - специалитет по специальности 40.05.03 «Судебная экспертиза»;

– Приказа Министерства образования и науки Российской Федерации № 499 от 01.07 2013 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Постановления Министерства труда и социального развития РФ от 21.08.1998 № 37 «Об утверждении Квалификационного справочника должностей руководителей, специалистов и других служащих» (с изменениями на 27 марта 2018 года).

1.2 Обоснование актуальности и практической значимости программы

Цифровая (телекоммуникационная) эпоха является как настоящим, так и перспективным будущим человека. Его повседневная деятельность с неизбежностью предполагает взаимодействие с устройствами и технологиями, которые стремительно меняют представление о реальности. Через аккаунты, свои цифровые «alter ego», человек коммуницирует, осуществляет трудовую деятельность, получает услуги, приобретает товары и др. В результате современный человек оказывается в положении параллельного бытия – физического и виртуального. Устраниться от этого, замедлить цифровизацию в известном смысле можно, но неизбежность и необратимость этого процесса в целом очевидна. Многие современные исследователи указывают на негативные последствия внедрения телекоммуникационных технологий с точки зрения состояния и динамики противоправной деятельности. Здесь, как правило, демонстрируется виртуализация механизма криминального оборота запрещенных предметов, что существенно осложнило деятельность правоохранительных органов. Кроме того, довольно обстоятельно раскрывается, что развитие отдельных направлений исследований (например, в сфере искусственного интеллекта и робототехники) обладает вполне конкретной угрозой для человечества в целом. Отдельно выделяется дегуманизирующее влияние цифровых технологий. Все приведенное в известном смысле справедливо. Однако верно и то, что дискурс этот в целом не выходит за рамки традиционного для человека замешательства перед чем-то новым, неизведанным, природа которого и возможное влияние представляются не до конца ясными. Любая технология имеет перспективу своей эксплуатации в преступных целях. Это, однако же, не может отменить прогресса как такового, то есть стремления человека к устройству своей жизни наиболее разумным (справедливым, безопасным, эффективным и т.п.) образом.

По этой причине надо говорить не о защите человека от технологий, а о построении модели защиты технологий или, если точнее, модели правового обеспечения информационно-телекоммуникационного развития, которая позволила бы упреждать и адекватно реагировать на совершение конкретного противоправного поведения.

Стратегией национальной безопасности Российской Федерации (Указ Президента РФ от 02.07.2021 № 400) развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия определены в числе национальных интересов государства. В Доктрине информационной безопасности Российской Федерации (Указ Президента Российской Федерации от 05.12.2016 № 646) (далее – Доктрина), Концепции информационной безопасности детей в Российской Федерации (Распоряжение Правительства РФ от 28.04.2023 № 1105-р, далее – Концепция), Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года (Указ Президента РФ от 17.05.2023 № 358, далее – Стратегия), Основах государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей (Указ Президента РФ от 09.11.2022 № 809, далее – Основы) отражены современные риски и угрозы информационной безопасности, в т.ч. следующие:

– пропаганда экстремистской идеологии, а также привлечение к террористической деятельности новых сторонников;

– вовлечение в деструктивные молодежные субкультуры, включая движения, связанные с вооруженным нападением на образовательные организации;

– размывание традиционных, в т. ч. семейных, ценностей;

– пропаганда совершения самоубийств и иного деструктивного поведения;

– пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ;

– провокация «психологического слома», следствием которого могут стать как депрессивное состояние, так и проявление девиантного поведения, повышенной агрессии к окружающим;

– навязывание представлений, предполагающих отрицание человеческого достоинства и ценности человеческой жизни;

– искажение исторической правды, разрушение исторической памяти и т.д.;

– распространение иной деструктивной информации.

В связи с этим существует социальный запрос на обучение и повышение квалификации специалистов, которые могут решать задачи в области противодействия противоправному поведению, совершаемому с использованием современных информационно-коммуникационных технологий, прежде всего, посредством распространения в сети «Интернет» противоправной информации.

Данная программа направлена на формирование у слушателей представлений о сущности и характеристике правонарушений, совершаемых с использованием информационно-коммуникационных технологий (далее – ИКТ), основных направлениях их предупреждения.

Программа рассмотрена и утверждена на заседании кафедры государственного и муниципального управления и политологии (протокол № 1 от 29 сентября 2025 г.).

1.3 Цель и задачи реализации программы

Целью реализации программы является повышение у слушателей профессиональных компетенций в области противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий.

Задачами курса являются:

– сформировать представление об административной ответственности в области информационно-коммуникационных технологий;

– осуществить анализ видов административных правонарушений в области информационно-коммуникационных технологий и особенностей их квалификации;

– сформировать представление о субъектах административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий;

– раскрыть особенности осуществления производства по делам об административных правонарушениях в области информационно-коммуникационных технологий;

– сформировать представление о понятии и видах преступлений, совершаемых с использованием информационно-коммуникационных технологий: понятие и виды;

– рассмотреть особенности уголовной ответственности за распространение информации в сети «Интернет», представляющей угрозу для жизни человека;

– изучить основания уголовной ответственности за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и распространение порнографии;

– изучить основы уголовно-правового противодействия терроризму и экстремизму в сети «Интернет»;

– проанализировать состояние, тенденции и детерминанты преступлений, совершаемых с использованием информационно-коммуникационных технологий;

– рассмотреть криминологическую характеристику лиц, совершающих преступления с использованием информационно-коммуникационных технологий;

– составить представление об основных направлениях криминологического противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

1.4 Формализованные результаты обучения

Слушатель, прошедший обучение по программе «Противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий», должен:

ЗНАТЬ	• основные и специальные понятия и закономерности формирования, функционирования и развития права в сфере противодействия правонарушениям, совершаемым с использованием ИКТ; • законодательство об административной ответственности за правонарушения с использованием информационно-коммуникационных технологий, особенности административных правонарушений в этой области, их виды и субъектный состав; • особенности привлечения к административной ответственности за совершение правонарушений с использованием информационно-коммуникационных технологий, виды и особенности применения к гражданам, должностным лицам и юридическим лицам административных наказаний, а также мер процессуального обеспечения и др.; • российское уголовное законодательство о преступлениях, совершаемых с использованием информационно коммуникационных технологий; • актуальные проблемы защиты информации уголовно-правовыми средствами.
УМЕТЬ	• оперировать административно-правовыми понятиями и категориями, анализировать юридические факты в сфере административной ответственности лиц, совершивших административные правонарушения с использованием

	информационно-коммуникационных технологий; • осуществлять правовую экспертизу нормативных и индивидуальных правовых актов в сфере использования информационно-коммуникационных технологий; • давать квалифицированные консультации; • правильно ставить вопросы, подлежащие разрешению в процессе привлечения лица, совершившего административное правонарушение с использованием информационно-коммуникационных технологий, к административной ответственности; • выявлять обстоятельства, способствовавшие совершению административных правонарушений с использованием информационно-коммуникационных технологий и др.; • правильно квалифицировать преступления, совершаемые с использованием информационно-коммуникационных технологий; • выявлять уголовно-правовые и криминологические риски в информационной сфере; • критически оценивать надежность источников информации, работает с противоречивой информацией из разных источников; • квалифицированно применять нормативные правовые акты в области правонарушений, совершаемых с использованием ИКТ, реализовывать нормы материального и процессуального права в профессиональной деятельности; • давать юридические заключения и консультации по вопросам уголовно-правовой охраны информации.
ВЛАДЕТЬ	• терминологией, связанной с уголовно-правовым и административно-правовым противодействием угрозам информационной безопасности; • навыками поиска, обобщения и анализа судебной практики по делам о правонарушениях, совершаемых с использованием информационно-коммуникационных технологий; • способностью формулировать выводы, содержащие ответы на поставленные вопросы, которые находят выражение в юридическом заключении или консультации по вопросам противодействия правонарушениям, совершаемым с использованием ИКТ; • методикой квалификации и разграничения различных видов правонарушений, совершаемых с использованием информационно-коммуникационных технологий, способностью разрешения проблем и коллизий в процессе правоприменения в рамках изучаемых вопросов; • терминологией, связанной с уголовно-правовым и криминологическим противодействием угрозам информационной безопасности;

	• навыками поиска, обобщения и анализа судебной практики по делам о преступлениях против информационной безопасности.

1.5 Формируемые компетенции и индикаторы их достижения

В приведенной ниже таблице перечисляются формулировки компетенций и индикаторы достижения компетенций, результаты обучения.

Разделы (темы) дисциплин (модуля)	**Код и наименование формируемых компетенций**	**Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля)**
Универсальные компетенции	**УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению **ИУК 1.3** Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников
	УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ
Общепрофессиональные компетенции	**ОПК-1** Способен анализировать нестандартные ситуации правоприменительной практики и предлагать оптимальные варианты их решения	**ИОПК 1.1** Знает основные и специальные понятия и закономерности формирования, функционирования и развития права; **ИОПК 1.2** Умеет самостоятельно анализировать нестандартные ситуации правоприменительной практики, выявлять, давать оценку; **ИОПК 1.3** Формулирует оптимальные пути решения нестандартной ситуации правоприменительной практики; **ИОПК 1.4** Владеет навыками принятия

		решений в нестандартных ситуациях правоприменительной практики с учетом этических принципов, норм и правил
	ОПК-3. Способен оперировать основными общеправовыми понятиями и категориями, анализировать и толковать нормы права, давать юридическую оценку фактам и обстоятельствам	**ИОПК-3.1** Обладает знаниями основных общеправовых понятий и категорий; **ИОПК-3.2** Обладает знаниями понятия, значения, видов, способов толкования нормы права; **ИОПК-3.3** Применяет знание законодательства при осуществлении толкования нормы права. **ИОПК-3.**4 Дает юридическую оценку фактам и обстоятельствам
	ОПК-7 Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	**ИОПК 7.1** Понимает принципы работы современных информационных технологий **ИОПК 7.2** Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности **ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности
Профессиональные компетенции	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам	**ИПК-1.1** Квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности; **ИПК-1.2** Квалифицированно толковать нормативные правовые акты; **ИПК-1.3.** Целенаправленно тренировать у себя профессиональное мышление
	ПК-2 Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать	**ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК-2.2** Понимает особенности различных форм реализации права **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение

	нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных

В приведенной ниже таблице перечисляются индикаторы достижения компетенций и результаты обучения по модулям.

Разделы (темы) дисциплины (модуля)	**Код и наименование формируемых компетенций**	**Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля)**
Модуль 1. «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»		
Тема 1.1. Административная ответственность в области информационно-коммуникационных технологий: понятие, характерные черты и принципы	**УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; **ИУК 1.3** Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ
Тема 1.2. Виды административных правонарушений в области информационно-коммуникационных технологий и особенности их	**ОПК-3.** Способен оперировать основными общеправовыми понятиями и категориями, анализировать и толковать нормы права, давать юридическую	**ИОПК-3.1** Обладает знаниями основных общеправовых понятий и категорий; **ИОПК-3.2** Обладает знаниями понятия, значения, видов, способов толкования нормы права; **ИОПК-3.3** Применяет знание законодательства при осуществлении

квалификации	оценку фактам и обстоятельствам; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	толкования нормы права; **ИОПК-3.4** Дает юридическую оценку фактам и обстоятельствам; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ
Тема 1.3. Субъекты административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий: понятие, виды, компетенция	**ОПК-3.** Способен оперировать основными общеправовыми понятиями и категориями, анализировать и толковать нормы права, давать юридическую оценку фактам и обстоятельствам; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИОПК-3.1** Обладает знаниями основных общеправовых понятий и категорий; **ИОПК-3.2** Обладает знаниями понятия, значения, видов, способов толкования нормы права; **ИОПК-3.3** Применяет знание законодательства при осуществлении толкования нормы права; **ИОПК-3.4** Даёт юридическую оценку фактам и обстоятельствам; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ
Тема 1.4. Производство по делам об административных правонарушениях.	**ОПК-1** Способен анализировать нестандартные ситуации правоприменительной практики и предлагать оптимальные варианты их решения; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИОПК 1.1** Знает основные и специальные понятия и закономерности формирования, функционирования и развития права; **ИОПК 1.2** Умеет самостоятельно анализировать нестандартные ситуации правоприменительной практики, выявлять, давать оценку; **ИОПК 1.3** Формулирует оптимальные пути решения нестандартной ситуации правоприменеиельной практики; **ИОПК 1.4** Владеет навыками принятия решений в нестандартных ситуациях правоприменительной практики с учетом этических принципов, норм и правил; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ

Модуль 2. «Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»		
Тема 2.1. Преступления, совершаемые с использованием информационно-коммуникационных технологий: понятие и виды	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права; **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права; **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Тема 2.2. Уголовная ответственность за распространение информации в сети «Интернет», представляющей угрозу для жизни человека («селфхарм»)	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК-1.1** Квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности; **ИПК-1.2** Квалифицированно толковать нормативные правовые акты; **ИПК-1.3.** Целенаправленно тренировать у себя профессиональное мышление **ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК-2.2** Понимает особенности различных форм реализации права **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права;

		ИПК-2.5 Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Тема 2.3. Уголовная ответственность за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и распространение порнографии	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК-1.1** Квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности; **ИПК-1.2** Квалифицированно толковать нормативные правовые акты; **ИПК-1.3.** Целенаправленно тренировать у себя профессиональное мышление; **ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Тема 2.4. Уголовно-правовое противодействие терроризму и	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам;	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ИПК-2.1** Знает правовые принципы и действующие нормативные правовые

экстремизму в сети «Интернет»	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права; **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Модуль 3. «Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»		
Тема 3.1. Состояние, тенденции и детерминанты преступлений, совершаемых с использованием информационно-коммуникационных технологий	**ОПК-7** Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности; **УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**ИОПК 7.1** Понимает принципы работы современных информационных технологий; **ИОПК 7.2** Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности; **ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности; **ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; **ИУК 1.3** Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников
Тема 3.2. Криминологическая	**ПК-2** Способен применять нормативные	**ИПК-2.1** Знает правовые принципы и действующие нормативные правовые

характеристика лиц, совершающих преступления с использованием информационно-коммуникационных технологий	правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права	акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права; **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права
Тема 3.3. Жертвы киберпреступлений	**УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий; **ОПК-7** Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	**ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; **ИУК 1.3** Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников; **ИОПК 7.1** Понимает принципы работы современных информационных технологий; **ИОПК 7.2** Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности; **ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности;
Тема 3.4. Основные направления криминологического противодействия преступлениям, совершаемым с использованием информационно-	**ОПК-7** Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной	**ИОПК 7.1** Понимает принципы работы современных информационных технологий; **ИОПК 7.2** Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности;

коммуникационных технологий	деятельности с учетом требований информационной безопасности **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных

1.6 Требования к уровню подготовки поступающего на обучение, необходимые для освоения программы

Лица, желающие освоить настоящую Программу, должны иметь высшее образование.

Объекты профессиональной деятельности: образовательные организации высшего образования, общеобразовательные организации, государственные организации, общественные институты, правоохранительные органы и силовые структуры, общественные организации (муниципальные, региональные, федеральные).

1.7 Трудоемкость обучения

Нормативная трудоемкость обучения по программе – **52 академических часа.**

1.8 Форма обучения

Форма обучения – очная.

1.9 Режим занятий

Учебная нагрузка устанавливается не более 36 часов в неделю, включая все виды аудиторной работы слушателя. Расписание составляется с учетом особенностей работы слушателей. Один академический час составляет 45 минут.

1.10 Срок обучения

Продолжительность обучения: не более одного месяца.

II. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план ДПОП ПК **«Противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»**

Продолжительность обучения - 52 часа.

№ п/п	Наименования модулей	Общая трудоемкость (час)	Аудиторные занятия (час)			Сам. работа
			Всего	Лекции	Практ. занятия, семинары	
1.	Модуль 1. «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»	18	12	8	4	6
2.	Модуль 2. «Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»	18	8	4	4	10
3.	Модуль 3. Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий	15	5	3	2	10
4.	Итоговая аттестация	**1**	**1**	-	-	-
5.	**Итого**	**52**	**26**	**15**	**10**	**26**

2.2. Учебно-тематический план

№ п/п	Наименования модулей и тем	Общая трудоемкость (час)	Аудиторные занятия (час)			Сам. работа	Формы текущего контроля
			Всего	Лекции	Прак. занятия		

1.	**Модуль 1. «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»**	**18**	**12**	**8**	**4**	**6**	
1.1.	**Тема 1.1.** Административная ответственность в области информационно-коммуникационных технологий: понятие, характерные черты и принципы	5	3	2	1	2	Устный опрос, тестирование
1.2.	**Тема 1.2.** Виды административных правонарушений в области информационно-коммуникационных технологий и особенности их квалификации	5	3	2	1	2	Устный опрос, тестирование
1.3.	**Тема 1.3.** Субъекты административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий: понятие, виды, компетенция	4	3	2	1	1	Устный опрос, тестирование
1.4.	**Тема 1.4.** Производство по делам об административных правонарушениях.	4	3	2	1	1	Устный опрос, тестирование
2.	**Модуль 2. «Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»**	**18**	**8**	**4**	**4**	**10**	
2.1.	**Тема 2.1**. Преступления, совершаемые с использованием информационно-коммуникационных	4	2	1	1	2	Устный опрос, тестирование

	технологий: понятие и виды						
2.2.	**Тема 2.2.** Уголовная ответственность за распространение информации в сети «Интернет», представляющей угрозу для жизни человека («селфхарм»)	6	2	1	1	4	Устный опрос, тестирование
2.3.	**Тема 2.3.** Уголовная ответственность за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и распространение порнографии	4	2	1	1	2	Устный опрос, тестирование
2.4.	**Тема 2.4.** Уголовно-правовое противодействие терроризму и экстремизму в сети «Интернет»	4	2	1	1	2	Устный опрос, тестирование
3.	**Модуль 3. Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий**	**15**	**5**	**3**	**2**	**10**	
3.1	**Тема 3.1.** Состояние, тенденции и детерминанты преступлений, совершаемых с использованием информационно-коммуникационных технологий	3	1	1	-	2	Устный опрос, тестирование
3.2	**Тема 3.2.** Криминологическая характеристика лиц, совершающих преступления с использованием информационно-коммуникационных технологий	6	2	1	1	4	Устный опрос, тестирование
3.3	**Тема 3.3.** Жертвы киберпреступлений	3	1	-	1	2	Устный опрос, тестирование

3.4	**Тема 3.4.** Основные направления криминологического противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий	3	1	1	-	2	Устный опрос, тестирование
4.	**Итоговая аттестация**	**1**	**1**				**Зачет**
5.	**Итого**	**52**	**26**	**15**	**10**	**26**	**26**

2.3. Описание модулей

2.3.1. Содержание модуля, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

Раздел (модуль) 1. «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»

№ п/п	Раздел, тема	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)				
		всего	Аудиторные уч. занятия		Сам. работа	Планируемые результаты обучения	Формы текущего контроля
			Лек.	Пр.			
1.1	**Тема 1.1.** Административная ответственность в области информационно-коммуникационных технологий: понятие, характерные черты и принципы	5	2	1	2	**УК-1, УК-4, ОПК-3**	Устный опрос, тестирование
1.2	**Тема 1.2.** Виды административных правонарушений в области информационно-коммуникационных технологий и особенности их квалификации	5	2	1	2		Устный опрос, тестирование

1.3	**Тема 1.3.** Субъекты административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий: понятие, виды, компетенция	4	2	1	1		Устный опрос, тестирование
1.4	**Тема 1.4.** Производство по делам об административных правонарушениях.	4	2	1	1		Устный опрос, тестирование
	Всего	**18**	**8**	**4**	**6**		

2.3.1.1. Виды занятий и их содержание

Рабочая программа Модуля 1 «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»

Цель модуля 1

Целью изучения модуля «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий» является формирование системного представления об административной ответственности за совершение правонарушений с использованием информационно-коммуникационных технологий, углубление знаний об особенностях применения компетентными государственными органам (должностными лицами и судьями) административно-правовых санкций к гражданам, должностным лицам и юридическим лицам, совершившим административное правонарушение с использованием информационно-коммуникационных технологий, приобретение компетенций, необходимых для последующей профессиональной правоприменительной, правозащитной деятельности в сфере ответственности за административные правонарушения, совершаемые с использованием информационно-коммуникационных технологий.

Задачи Модуля 1:

- формирование представлений о правовых и фактических основаниях привлечения граждан, должностных лиц и юридических лиц, виновных в совершении административных правонарушений с использованием информационно-коммуникационных технологий, к административной ответственности;

- приобретение знаний о содержании и особенностях порядка привлечения к административной ответственности за нарушения, связанные с использованием информационно-коммуникационных технологий;

- приобретение знаний о компетенции уполномоченных органов исполнительной власти, их должностных лиц и судей по привлечению к административной ответственности за совершение административных правонарушений с использованием информационно-коммуникационных технологий;

- приобретение знаний о различных видах административных наказаний, применяемых за совершение административных правонарушений с использованием информационно-коммуникационных технологий;

- формирование навыков квалифицированного применения нормативных правовых актов, регламентирующих вопросы административной ответственности за правонарушения с использованием информационно-коммуникационных технологий.

Содержание Модуля 1 «Административно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»

Тема 1.1 Административная ответственность в области информационно-коммуникационных технологий: понятие, характерные черты и принципы

Область информационно-коммуникационных технологий как объект административно-правового регулирования. Административная ответственность в области информационно-коммуникационных технологий: понятие, признаки, правовое регулирование. Принципы административной ответственности в области информационно-коммуникационных технологий.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 1.2 Виды административных правонарушений в области информационно-коммуникационных технологий и особенности их квалификации

Нарушение правил защиты информации (ст. 13.12 КоАП РФ). Нарушения требований в области обеспечения безопасности критической информационной инфраструктуры (ст. 13.12.1 КоАП РФ). Административные правонарушения, связанные с деятельностью средств массовой информации (ст. ст. 13.15, 13.15.1, 13.16, ч. 1. 2.1, 3 ст. 13.21, 13.22 КоАП РФ). Административные правонарушения, связанные с посягательством на информационную безопасность несовершеннолетних.

Нарушение законодательства о защите детей от информации, причиняющей вред их здоровью и (или) развитию ст. 6.17, ч. 2 ст. 13.21 КоАП РФ. Административные нарушения, связанные с пропагандой нетрадиционных сексуальных отношений среди несовершеннолетних (ст. 6.21 КоАП РФ). Административные правонарушения, связанные с распространением экстремистских материалов среди несовершеннолетних (ч.3 ст.13.41 КоАП РФ, ст. ст. 20.3,20.29 КоАП РФ). Административные правонарушения, связанные с распространением террористической идеологии среди несовершеннолетних (ч.1 ст. 13.37 КоАП РФ). Административные правонарушения, связанные с распространением информации о наркотиках среди несовершеннолетних (ч.1 ст.6.13 КоАП РФ, ч.3 ст. 13.41 КоАП РФ). Административные правонарушения, связанные с привлечением несовершеннолетних к порнографической деятельности и их эксплуатации в сексуальных целях (ст. 6.20, ч.ч. 2, 4 ст.6.21 КоАП РФ). Административные правонарушения, связанные с торговлей наркотиками в Интернете (ст. 6.8, ч.1.1 ст. 6.13, ст. 6.16.1 КоАП РФ). Административно-наказуемые действия с компьютерной информацией ограниченного доступа (ч. 1 2, 4-6 ст.13.41 КоАП РФ).

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 1.3 Субъекты административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий: понятие, виды, компетенция

Понятие и виды субъектов административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий. Подведомственность дел об административных правонарушениях в области информационно-коммуникационных технологий. Административно-юрисдикционные полномочия Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Административно-юрисдикционные полномочия Федеральной службы безопасности Российской Федерации (ФСБ России). Административно-юрисдикционные полномочия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Судьи судов общей юрисдикции как субъекты административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 1.4 Производство по делам об административных правонарушениях.

Понятие и принципы производства по делам об административных правонарушениях. Понятие и назначение стадии возбуждения дела об административном правонарушении в области информационно-коммуникационных технологий. Поводы, основание и формы возбуждения дела об административном правонарушении. Административное расследование по делу об административном правонарушении в области информационно-коммуникационных технологий: понятие, содержание, основания назначения, порядок и сроки проведения. Протокол об административном правонарушениях как акт возбуждения дела об административном правонарушении области использования информационно-коммуникационных технологий. Сроки составления протокола, требования, предъявляемые к его форме и содержанию. Существенные недостатки протокола об административном правонарушении, их правовые последствия и способы устранения. Должностные лица, уполномоченные составлять протоколы об административных правонарушениях в области информационно-коммуникационных технологий. Полномочия должностных лиц ФСТЭК России. Полномочия должностных лиц ФСБ России. Полномочия должностных лиц Роскомнадзора. Полномочия должностных лиц органов внутренних дел. Полномочия должностных лиц военной полиции Вооруженных Сил Российской Федерации. Полномочия должностных лиц Федеральной службы по надзору сфере здравоохранения (Росздравнадзор). Полномочия прокурора. Основания прекращения производства по делу об административном правонарушении в области информационно-коммуникационных технологий на стадии возбуждения дела.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

2.3.1.2. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Разделы (темы) дисциплины (модуля)	Код и наименование формируемых компетенций	Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля)

Тема 1.1. Административная ответственность в области информационно-коммуникационных технологий: понятие, характерные черты и принципы	**УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; **ИУК 1.3** Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ
Тема 1.2. Виды административных правонарушений в области информационно-коммуникационных технологий и особенности их квалификации	**ОПК-3.** Способен оперировать основными общеправовыми понятиями и категориями, анализировать и толковать нормы права, давать юридическую оценку фактам и обстоятельствам; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИОПК-3.1** Обладает знаниями основных общеправовых понятий и категорий; **ИОПК-3.2** Обладает знаниями понятия, значения, видов, способов толкования нормы права; **ИОПК-3.3** Применяет знание законодательства при осуществлении толкования нормы права; **ИОПК-3.4** Дает юридическую оценку фактам и обстоятельствам; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ
Тема 1.3. Субъекты административной юрисдикции по делам об административных правонарушениях в области информационно-коммуникационных технологий: понятие, виды, компетенция	**ОПК-3.** Способен оперировать основными общеправовыми понятиями и категориями, анализировать и толковать нормы права, давать юридическую оценку фактам и обстоятельствам; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для	**ИОПК-3.1** Обладает знаниями основных общеправовых понятий и категорий; **ИОПК-3.2** Обладает знаниями понятия, значения, видов, способов толкования нормы права; **ИОПК-3.3** Применяет знание законодательства при осуществлении толкования нормы права; **ИОПК-3.4** Даёт юридическую оценку фактам и обстоятельствам; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на

	академического и профессионального взаимодействия	государственном языке РФ
Тема 1.4. Производство по делам об административных правонарушениях.	**ОПК-1** Способен анализировать нестандартные ситуации правоприменительной практики и предлагать оптимальные варианты их решения; **УК-4** Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	**ИОПК 1.1** Знает основные и специальные понятия и закономерности формирования, функционирования и развития права; **ИОПК 1.2** Умеет самостоятельно анализировать нестандартные ситуации правоприменительной практики, выявлять, давать оценку; **ИОПК 1.3** Формулирует оптимальные пути решения нестандартной ситуации правоприменительной практики; **ИОПК 1.4** Владеет навыками принятия решений в нестандартных ситуациях правоприменительной практики с учетом этических принципов, норм и правил; **ИУК-4.1** Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ

2.3.1.3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.

Общая трудоемкость (объем) (модуля) составляет 18 академических часов.

Объём модуля	Всего часов
Общая трудоемкость модуля	18
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	
Аудиторная работа (всего):	12
в том числе:	
лекции	8
семинары, практические занятия	4
практикумы	Не предусмотрено
лабораторные работы	Не предусмотрено
Внеаудиторная работа:	
консультация перед зачетом	-
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподавателем, групповые, индивидуальные консультации и иные виды учебной	

деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем), творческую работу (эссе), рефераты, контрольные работы и др.	
Самостоятельная работа	6
Вид промежуточной аттестации обучающегося (зачет / экзамен)	-

2.3.2. Содержание модуля, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

Раздел (модуль) 2. «Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»

№ п/п	Раздел, тема	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)				
		всего	Аудиторные уч. занятия		Сам. работа	Планируемые результаты обучения	Формы текущего контроля
			Лек.	Пр.			
2.1	**Тема 2.1**. Преступления, совершаемые с использованием информационно-коммуникационных технологий: понятие и виды	4	1	1	2	ПК-1, ПК-3	Устный опрос, тестирование
2.2	**Тема 2.2.** Уголовная ответственность за распространение информации в сети «Интернет», представляющей угрозу для жизни человека («селфхарм»)	6	1	1	4		Устный опрос, тестирование
2.3	**Тема 2.3.** Уголовная ответственность за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и	4	1	1	2		Устный опрос, тестирование

	распространение порнографии						
2.4	**Тема 2.4.** Уголовно-правовое противодействие терроризму и экстремизму в сети «Интернет»	4	1	1	2		Устный опрос, тестирование
	Всего	**18**	**4**	**4**	**10**		

2.3.2.1. Виды занятий и их содержание

Рабочая программа Модуля 2. «Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»

Цель освоения Модуля 2

Целью изучения модуля «Уголовно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий» является формирование у слушателей компетенций в области уголовно-правовой квалификации преступных деяний, совершаемых с использованием современных информационно-коммуникационных технологий.

Задачи Модуля 2:

– сформировать представление о понятии и видах преступлений, совершаемых с использованием информационно-коммуникационных технологий: понятие и виды;

– рассмотреть особенности уголовной ответственности за распространение информации в сети «Интернет», представляющей угрозу для жизни человека («селфхарм»);

– изучить основания уголовной ответственности за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и распространение порнографии;

– изучить основы уголовно-правового противодействия терроризму и экстремизму в сети «Интернет».

Содержание Модуля 2 «Уголовно-правовое противодействие правонарушениям, совершаемым с использованием информационно-коммуникационных технологий»

Тема 2.1. Преступления, совершаемые с использованием информационно-коммуникационных технологий: понятие и виды

Понятие информационной безопасности в современном мире. Цифровая экономика как самостоятельный объект уголовно-правовой охраны. Социальная обусловленность уголовно-правовой охраны информационной безопасности. Основные подходы к определению преступлений против

информационной безопасности. Виды преступлений против информационной безопасности. Преступления против информационной безопасности в широком и узком смысле. Компьютерные и компьютеризированные преступления. Криптовалютные преступления.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 2.2. Уголовная ответственность за распространение информации в сети «Интернет», представляющей угрозу для жизни человека («селфхарм»)

Селфхарм. Суицидальный контент: склонение к совершению самоубийства или содействие совершению самоубийства (110^1 УК); организация деятельности, направленной на побуждение к совершению самоубийства(110^2 УК) Несуицидаотный контент. Опасные игры (Зажечь не по-детски, Исчезни на сутки, Руффинг, Зацепинг и т.п). Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (151^2 УК)

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 2.3. Уголовная ответственность за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и распространение порнографии

Преступления, посягающие на половую неприкосновенность несовершеннолетних: насильственные (131, 132,133 УК РФ) и ненасильственные (134, 135 УК). Влияние возраста потерпевшего на квалификацию. Получение сексуальных услуг несовершеннолетнего (240.1 УК РФ). Понятие порнографии. Отграничение порнографии от иного контента, содержащего информацию негативно влияющую на нравственное здоровье несовершеннолетних. Киберпроституция. Вебкам. Незаконные изготовление и оборот порнографических материалов или предметов. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 2.4. Уголовно-правовое противодействие терроризму и экстремизму в сети «Интернет»

Понятие терроризма и экстремизма. Кибертерроризм. Основные виды угроз экстремистского характера в медиасреде и их отличительные черты. Противодействие вовлечению в преступления террористической и экстремистской направленности. Особенности вовлечения лиц в террористическую и экстремистскую деятельность с использованием современных информационных технологий. Противодействие распространению в сети Интернет материалов, направленных на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе. Героизация нацистских преступников в медиасреде.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

2.3.2.2. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Разделы (темы) дисциплины (модуля)	Код и наименование формируемых компетенций	Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля)
Тема 2.1. Преступления, совершаемые с использованием информационно-коммуникационных технологий: понятие и виды	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права; **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права; **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права;

		ИПК-3.1 Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Тема 2.2. Уголовная ответственность за распространение информации в сети «Интернет», представляющей угрозу для жизни человека («селфхарм»)	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ИПК-1.1** Квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности; **ИПК-1.2** Квалифицированно толковать нормативные правовые акты; **ИПК-1.3.** Целенаправленно тренировать у себя профессиональное мышление **ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права **ИПК-2.2** Понимает особенности различных форм реализации права **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Тема 2.3. Уголовная ответственность за посягательства на половую неприкосновенность несовершеннолетних, совершаемые в сети «Интернет», и распространение	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ПК-2** Способен применять нормативные правовые акты в соответствующих сферах	**ИПК-1.1** Квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности; **ИПК-1.2** Квалифицированно толковать нормативные правовые

порнографии	профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	акты; **ИПК-1.3.** Целенаправленно тренировать у себя профессиональное мышление; **ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных
Тема 2.4. Уголовно-правовое противодействие терроризму и экстремизму в сети «Интернет»	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	**ПК-1** Квалификация фактов, событий и обстоятельств по уголовным делам; **ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права; **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач

		на основе норм права и полученных аналитических данных

2.3.2.3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.

Общая трудоемкость (объем) (модуля) составляет 18 академических часов.

Объём модуля	Всего часов
Общая трудоемкость модуля	18
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	
Аудиторная работа (всего):	8
в том числе:	
лекции	4
семинары, практические занятия	4
практикумы	Не предусмотрено
лабораторные работы	Не предусмотрено
Внеаудиторная работа:	
консультация перед зачетом	-
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподавателем, групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем), творческую работу (эссе), рефераты, контрольные работы и др.	
Самостоятельная работа	10
Вид промежуточной аттестации обучающегося (зачет / экзамен)	-

2.3.3. Содержание модуля, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.

Раздел (модуль) 3. Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий

№ п/п	Раздел, тема	Общая трудоемкость (в часах)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)

		всего	Аудиторные уч. занятия		Сам. работа	Планируемые результаты обучения	Формы текущего контроля
			Лек.	Пр.			
2.1	**Тема 3.1.** Состояние, тенденции и детерминанты преступлений, совершаемых с использованием информационно-коммуникационных технологий	3	1	-	2	**УК-1, ОПК-7, ПК-3**	Устный опрос, тестирование
2.2	**Тема 3.2.** Криминологическая характеристика лиц, совершающих преступления с использованием информационно-коммуникационных технологий	6	1	1	4		Устный опрос, тестирование
2.3	**Тема 3.3.** Жертвы киберпреступлений	3	-	1	2		Устный опрос, тестирование
2.4	**Тема 3.4.** Основные направления криминологического противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий	3	1	-	2		Устный опрос, тестирование
	Всего	**15**	**3**	**2**	**10**		

4.3. Рабочая программа Модуля 3 «Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»

Цели и задачи Модуля 3

Целью изучения модуля «Криминологическое противодействие правонарушениям, совершаемым с использованием информационно-

коммуникационных технологий» является формирование у слушателей компетенций в области криминологического анализа и противодействия преступности, совершаемой с использованием информационно-коммуникационных технологий.

Задачи Модуля 3:

– сформировать представления о понятии и видах преступности, совершаемой с использованием информационно-коммуникационных технологий;

– рассмотреть криминологическую характеристику основных статистических показателей, отражающих состояние и тенденции преступности, совершаемой с использованием информационно-коммуникационных технологий;

– определить совокупность криминогенных факторов, детерминирующих преступность, совершаемую с использованием информационно-коммуникационных технологий;

– рассмотреть криминологическую характеристику лиц, совершающих преступления с использованием информационно-коммуникационных технологий и жертв киберпреступлений;

– изучить основные направления криминологического противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

Содержание Модуля 3 «Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»

Тема 3.1. Состояние, тенденции и детерминанты преступлений, совершаемых с использованием информационно-коммуникационных технологий

Понятие преступлений, совершаемых с использованием информационно-коммуникационных технологий. Понятие киберпреступности и киберпреступления. Состояние, структура и тенденции преступности в сфере информационно-коммуникационных технологий. Криминологическая характеристика отдельных видов киберпреступности. Криминологическая (криминогенная и антикриминогенная) детерминация преступности в сфере информационно-коммуникационных технологий. Причины и условия отдельных видов киберпреступности. Самодетерминация

киберпреступности. Латентность киберпреступности. Общая характеристика киберпреступности зарубежных стран.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 3.2. Криминологическая характеристика лиц, совершающих преступления с использованием информационно-коммуникационных технологий

Понятие и структура личности киберпреступника. Классификация и типология личности киберпреступника. Место и роль личности киберпреступника в механизмах совершения киберпреступлений. Влияние личностных факторов на киберпреступность.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 3.3. Жертвы киберпреступлений

Виктимологическая характеристика личности потерпевшего от преступлений в сфере информационно-коммуникационных технологий. Классификация и типология жертв киберпреступлений. Место и роль личности потерпевшего в механизмах совершения киберпреступлений.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

Тема 3.4. Основные направления криминологического противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Основы организации системы противодействия преступлениям в сфере информационно-телекоммуникационных технологий. Современное правовое обеспечение кибербезопасности в России. Субъекты противодействия киберпреступности. Общие меры противодействия киберпреступности.

Специальные меры противодействия киберпреступности. Меры виктимологической профилактики. Современные информационные решения применяемые в киберпространстве, как средства совершения киберпреступлений и средства их пресечения (блокчейн, криптовалюты, нейросети, искусственный интеллект). Международно-правовое обеспечение кибербезопасности и международно-правовое сотрудничество в сфере информационно-коммуникационных технологий.

Формат занятия – лекция.

Внеаудиторные занятия – самостоятельная работа.

Задания для самостоятельной работы:

– провести самостоятельное исследование раскрытых в материалах вопросов с использованием рекомендованной литературы.

2.3.2.3. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Разделы (темы) дисциплины (модуля)	Код и наименование формируемых компетенций	Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля)
Модуль 3. «Криминологическое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий»		
Тема 3.1. Состояние, тенденции и детерминанты преступлений, совершаемых с использованием информационно-коммуникационных технологий	**ОПК-7** Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности; **УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**ИОПК 7.1** Понимает принципы работы современных информационных технологий; **ИОПК 7.2** Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности; **ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности; **ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; **ИУК 1.3** Критически оценивает надежность источников информации,

		работает с противоречивой информацией из разных источников
Тема 3.2. Криминологическая характеристика лиц, совершающих преступления с использованием информационно-коммуникационных технологий	**ПК-2** Способен применять нормативные правовые акты в соответствующих сферах профессиональной деятельности, реализовывать нормы материального права	**ИПК-2.1** Знает правовые принципы и действующие нормативные правовые акты с учетом специфики отдельных отраслей права; **ИПК-2.2** Понимает особенности различных форм реализации права; **ИПК-2.3** Устанавливает фактические обстоятельства, имеющие юридическое значение; **ИПК-2.4** Определяет характер правоотношения и подлежащие применению нормы материального права; **ИПК-2.5** Принимает обоснованные юридические решения и оформляет их в точном соответствии с нормами материального и процессуального права
Тема 3.3. Жертвы киберпреступлений	**УК-1** Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий; **ОПК-7** Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	**ИУК 1.1** Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; **ИУК 1.2** Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; **ИУК 1.3** Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников; **ИОПК 7.1** Понимает принципы работы современных информационных технологий; **ИОПК 7.2** Умеет выбрать современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности; **ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности;
Тема 3.4. Основные направления криминологического противодействия	**ОПК-7** Способен применять информационные технологии и	**ИОПК 7.1** Понимает принципы работы современных информационных технологий; **ИОПК 7.2** Умеет выбрать

преступлениям, совершаемым с использованием информационно-коммуникационных технологий	использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности **ПК-3** Способен давать юридические консультации и заключения в различных сферах юридической деятельности	современные информационные технологии, необходимые для решения конкретных задач профессиональной деятельности; **ИОПК 7.3** Владеет навыками использования современных информационных технологий, необходимыми для решения конкретных задач профессиональной деятельности; **ИПК-3.1** Выявляет и формулирует наличие правовой проблемы; **ИПК-3.2** Вырабатывает различные варианты решения конкретных задач на основе норм права и полученных аналитических данных

2.3.2.3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.

Общая трудоемкость (объем) (модуля) составляет 15 академических часов.

Объём модуля	Всего часов
Общая трудоемкость модуля	15
Контактная работа обучающихся с преподавателем (по видам учебных занятий)* (всего)	
Аудиторная работа (всего):	5
в том числе:	
лекции	3
семинары, практические занятия	2
практикумы	Не предусмотрено
лабораторные работы	Не предусмотрено
Внеаудиторная работа:	
консультация перед зачетом	-
Внеаудиторная работа также включает индивидуальную работу обучающихся с преподавателем, групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем), творческую работу (эссе), рефераты, контрольные работы и др.	
Самостоятельная работа	10
Вид промежуточной аттестации обучающегося (зачет / экзамен)	-

III. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1 Материально-технические условия реализации программы

Для реализации программы используются помещения, представляющие собой учебные аудитории для проведения всех видов учебных занятий, предусмотренных учебным планом, оснащенные оборудованием и техническими средствами обучения.

Наименование специализированных аудиторий кабинетов, лабораторий (адрес)	**Вид занятий**	**Наименование оборудования/программного обеспечения**
Диссертационный зал № 504 (ул. Ленина, 29, учебно-лабораторный корпус, 5 этаж)	Лекции, практические занятия, групповые и индивидуальные консультации, итоговая аттестация	Специализированная мебель: столы, конференц-кресла. Технические средства обучения: WWeb-камера AVERMEDIA PW; аудио-видео конференц-система (многозадачная камера Panasonic; устройство захвата Epiphan Lecture Recorder x2, мультимедийный экран (Dell S2240T; матричный интерфейс Kramer VC-44HN; потолочная акустическая система Audac Ceio8), усилитель); ноутбук мультимедийный ASUS ROG GL552VW Core i5 4Core, 8Gb ОЗУ, 1Tb Hdd с подключением к информационно-телекоммуникационной сети «Интернет»; проектор BenQ Proektor SH 940. Лицензионное программное обеспечение: – Microsoft Windows (Лицензия № 60290784), бессрочная; – Microsoft Office (Лицензия № 60127446), бессрочная; – ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная; – Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная; – Google G Suite for Education (IC: 01i1p5u8), бессрочная; – Kaspersky Endpoint Security (Лицензия № 1CI2-230131-040105-990-2679), с 21.01.2023 по 03.03.2025.
Компьютерный класс № 417 (ул. Ленина, 29, учебный корпус № 3, 4 этаж)	Лекции, практические занятия, лабораторные работы,	Специализированная мебель: столы компьютерные, кресла оператора, стол конференционный, доска маркерная. Технические средства обучения:

	групповые и индивидуальные консультации, текущий контроль и промежуточная аттестация	12 персональных компьютеров с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, 12 комплектов видео-конференц связи. Лицензионное программное обеспечение: - Microsoft Windows (Лицензия № 60290784), бессрочная; - Microsoft Office (Лицензия № 60127446), бессрочная; - ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная; - Calculate Linux (внесѐн в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная; - Google G Suite for Education (IC: 01i1p5u8), бессрочная; - Kaspersky Endpoint Security (Лицензия № 1CE2-230131-040105-990-2679), с 31.01.2023 по 03.03.2025; - Антивирус Касперского. Действует до 03.03.2025г. (Договор № 56/2023 от 25 января 2023 г.); - пакет приложений для объектно-ориентированного программирования Embarcadero (Item Number: 2013123054325206. Срок действия лицензии: бессрочная); - пакет визуального редактирования растровых изображений GIMP (Лицензия № GNU GPLv3, бессрочная); - образовательная подписка Google G Suite for Education (видеоконференции, дневник, календарь, диск и прочее). (Срок действия лицензии: бессрочная); - пакет математического моделирования Mathcad (Contract Number (SCN) 4A1913127. Срок действия лицензии: бессрочная); - система поиска заимствований в текстах «Антиплагиат ВУЗ» (Договор № 3262 от 20.01.2021); - Информационно-правовая система «Инофрмио» (Договор № НК 1017 от 20.01.2021); - пакет визуального 3D-моделтрования Blender (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная); - векторный графический редактор Inkscape (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная); - программный комплекс для верстки Scribus (Лицензия № GNU GPL v3. Срок действия лицензии: бессрочная);

		- Autodesk AutoCAD (Лицензия № 5X6-30X999XX. Бессрочная образовательная (академическая) лицензия); - Autodesk 3DS Max (Лицензия № 5X5-93X928XX. Бессрочная образовательная (академическая) лицензия); - Autodesk Revit (Лицензия № 5X6-03X109XX. Бессрочная образовательная (академическая) лицензия)

1. Научный зал, 20 мест, 10 компьютеров (учебно-лабораторный корпус, ауд.101)

Специализированная мебель: столы ученические, стулья.

Технические средства обучения:

персональные компьютеры с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Лицензионное программное обеспечение:

– Microsoft Windows (Лицензия № 60290784), бессрочная;

– Microsoft Office (Лицензия № 60127446), бессрочная;

– ABBY Fine Reader (лицензия № FCRP-1100-1002-3937), бессрочная;

– Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная;

– Google G Suite for Education (IC: 01i1p5u8), бессрочная;

– Kaspersky Endpoint Security (лицензия № 1CI2-230131-040105-990-2679), с 21.01.2023 по 03.03.2025.

2. Читальный зал, 80 мест, 10 компьютеров (учебно-лабораторный корпус, ауд. 102а).

Специализированная мебель: столы ученические, стулья.

Технические средства обучения:

Дисплей Брайля ALVA с программой экранного увеличителя MAGic Pro;

стационарный видеоувеличитель CIear View с монитором;

2 компьютерных роллера USB&PS/2; клавиатура с накладкой (ДЦП);

акустическая система свободного звукового поля Front Row to Go/$;

персональные компьютеры с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Лицензионное программное обеспечение:

– Microsoft Windows (Лицензия № 60290784), бессрочная;

– Microsoft Office (Лицензия № 60127446), бессрочная;

– ABBY Fine Reader (лицензия № FCRP-1100-1002-3937),

бессрочная;

– Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная;

– Google G Suite for Education (IC: 01i1p5u8), бессрочная;

– Kaspersky Endpoint Security (лицензия № 1CI2-230131-040105-990-2679), с 21.01.2023 по 03.03.2025.

Необходимый комплект лицензионного программного обеспечения

1. ABBY FineReader (лицензия №FCRP-1100-1002-3937), бессрочная.
2. Calculate Linux (внесён в ЕРРП Приказом Минкомсвязи №665 от 30.11.2018-2020), бессрочная.
3. Google G Suite for Education (IC: 01i1p5u8), бессрочная.
4. Kaspersky Endpoint Security (лицензия № 1CI2-230131-040105-990-2679), с 21.01.2023 по 03.03.2025.
5. Microsoft Office (лицензия №60127446), бессрочная.
6. Microsoft Windows (лицензия №60290784), бессрочная.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде (далее - ЭИОС) Университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее. Для каждого слушателя создается логин и пароль для осуществления процедуры освоения знаний и навыков по дисциплинам учебного плана в ЭИОС ФГБОУ ВО «КЧГУ».

Адрес официального сайта университета: http://kchgu.ru.

Адрес размещения ЭИОС ФГБОУ ВО «КЧГУ»: https://do.kchgu.ru.

Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин и подлежит обновлению (при необходимости).

3.2 Современные профессиональные базы данных

1. Федеральный портал «Российское образование»- https://edu.ru/documents/
2. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) - http://school-collection.edu.ru/
3. Базы данных Scopus издательства Elsevir http://www.scopus.com/search/form.uri?displav=basi .
4. Гарант. Информационно-правовая база- www.garant.ru

3.3 Информационные справочные системы

1. Портал Федеральных государственных образовательных стандартов высшего образования- http://fgosvo.ru.
2. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) - http://edu.ru.
3. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ИДР) - http://school-collection.edu.ru
4. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») - http://window/edu.ru.
5. Российская государственная библиотека- http://www.rsl.ru
6. Государственная публичная историческая библиотека- http://www.shpi.ru

3.4 Электронно-библиотечные системы (электронные библиотеки)

1. Электронная библиотечная система «Знаниум». https://znanium.com.
2. Современная электронная библиотека «Лань» https://e.lanbook.com .
3. Научная электронная библиотека «ELIBRARY.RU» - https://www.elibrary.ru.
4. Национальная электронная библиотека (НЭБ) - https://rusneb.ru.
5. Электронный ресурс Polred.com Обзор СМИ - https://polpred.com ,
6. Электронная библиотека КЧГУ - http://lib.kchgu.ru.

Библиотека университета располагает достаточным количеством экземпляров рекомендуемой в качестве обязательной учебной и учебно-методической литературы по дисциплинам учебных планов. Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

3.5. Учебно-методическое обеспечение программы

3.5.1Основная литература

1. Административное право : учебник / под ред. Л.Л. Попова, М.С. Студеникиной. — 3-е изд., перераб. и доп. — Москва : Норма : ИНФРА-М, 2024. — 736 с. - ISBN 978-5-00156-083-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2010481 (дата обращения: 13.05.2025)
2. Выявление и профилактика деструктивной пропаганды в молодежной и подростковой среде: методическое пособие / под ред. В.Д. Никишина. М.: Издательство «Первый том», 2021. 136 с.

3. Галяшина Е. И., Никишин В. Д. Информационно-мировоззренческая безопасность в интернет-медиа: монография. М.: Проспект, 2023. 424 с.

4. Мигачев, Ю. И. Административное право Российской Федерации : учебник для вузов / Ю. И. Мигачев, Л. Л. Попов, С. В. Тихомиров ; под редакцией Л. Л. Попова. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 456 с. — (Высшее образование). — ISBN 978-5-534-08218-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510449 (дата обращения: 13.05.2025).

5. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения. М.: ИНФРА-М, 2023. 351 с.

6. Уголовное право России. Части Общая и Особенная : учебник / под ред. А. И. Рарога. 10-е изд., перераб. и доп. – М.: Проспект, 2020. 944 с.

7. Юрченко И. А. Преступления против информационной безопасности: учебное пособие. – Москва: Проспект, 2021. – 208 с.

3.5.2 Нормативные правовые акты (в действующей редакции)

Конституция Российской Федерации, принятая народным голосованием 12 декабря 1993 г. (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (Дата обращения: 20.03.2025).

Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (Дата обращения: 20.03.2025).

Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/cons_doc_LAW_34661/ (Дата обращения: 20.03.2025).

Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW108808/ (Дата обращения: 20.03.2025).

Федеральный закон «О наркотических средствах и психотропных веществах» от 08.01.1998 № 3-ФЗ (последняя редакция) // [Электронный ресурс]

КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW17437/ (Дата обращения: 20.03.2025).

Федеральный закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW58840/ (Дата обращения: 20.03.2025).

Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW37867/ (Дата обращения: 20.03.2025).

Федеральный закон «О свободе совести и о религиозных объединениях» от 26.09.1997 № 125-ФЗ (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW16218/ (Дата обращения: 20.03.2025).

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW61798/ (Дата обращения: 20.03.2025).

Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации» от 23 июня 2016 № 182-ФЗ (последняя редакция) // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: ttps://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=199976&cacheid=972582AD2E706F45C8E7968B244AAADC&mode=splus&rnd=e9x28CUExCDtYbbf#Rgy28CU33ik6a2h9 / (Дата обращения: 20.03.2025).

Федеральный закон «О ратификации соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» от 1 октября 2008 № 164-ФЗ// [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=80371&cacheid=5804993DD55239A52A94B28DD313B46B&mode=splus&rnd=e9x28CUExCDtYbbf#cin38CUrp5U6j1QB (Дата обращения: 20.03.2025).

Закон РФ от 27.12.1991 № 2124-1 (ред. от 13.06.2023) «О средствах массовой информации» // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW58840/ (Дата обращения: 20.03.2025).

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW208191/ (Дата обращения: 20.03.2025).

Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW216363/ (Дата обращения: 20.03.2025).

Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW389271/ (Дата обращения: 20.03.2025).

Постановление Правительства РФ от 26.10.2012 № 1101 (ред. от 29.04.2023) «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (вместе с «Правилами создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», «Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети «Интернет», распространение которых в Российской Федерации запрещено») // [Электронный ресурс] КонсультантПлюс: справ. правовая система // URL: http://www.consultant.ru/document/consdocLAW137077/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (Дата обращения: 20.03.2025).

Судебная практика

Постановления Пленума Верховного суда РФ. – URL: http://www.vsrf.ru/documents/own/, http://www.consultant.ru/.

Судебная практика по конкретным делам: сайт Судебные и нормативные акты РФ. – URL: http://sudact.ru

3.5.3 Дополнительная литература

Амелина Я. А. «Группы смерти» как угроза национальной безопасности России. Аналитический доклад (18+) / Кавказский геополитический клуб. М.: Издатель А.В. Воробьев, 2017. 76 с.

Аналитический обзор с предложениями «Механизмы противодействия органов внутренних дел (полиции) государств – участников СНГ вовлечению несовершеннолетних в деструктивные группы в сети Интернет»/ФГКУ «ВНИИ МВД Российской Федерации». М., 2021.72 с.

Артюшина О. В. Организация деятельности, направленной на побуждение к суицидальному поведению, как новелла уголовного закона // Уголовное право. 2019. № 5. С. 10 – 15.

Бычкова А. М., Раднаева Э. Л. Доведение до самоубийства посредством использования интернет-технологий: социально-психологические, криминологические и уголовно-правовые аспекты // Всероссийский криминологический журнал. 2018. № 1. С. 101 – 115.

Воронин В. Н. Уголовно-правовые риски развития цифровых технологий: постановка проблемы и методы научного исследования // Вестник Университета имени О.Е. Кутафина. 2018. № 12. С. 73-80.

Галяшина Е. И., Никишин В. Д. Деструктивное речевое поведение в цифровой среде: факторы, детерминирующие негативное воздействие на мировоззрение пользователя // Lex russica. 2021. Т. 74. № 6. С. 79 – 94. – DOI: 10.17803/1729-5920.2021.175.6.078-093.

Гончаров Л. А. Колумбайн и скулшутинг в структуре молодежного экстремизма и терроризма // Вестник Воронежского института экономики и социального управления. 2019. №2. С. 29 – 31.

Дамаскин О. В., Красинский В. В. Криминологическая характеристика механизма вовлечения несовершеннолетних в противоправную деятельность // Государство и право. 2020. № 8. С. 41 – 54.

Джафарли В.Ф. Формирование и развитие системы криминологической безопасности в сфере информационно - коммуникационных технологий: дис. ... д-ра юрид. наук: 5.1.4. / Джафарли Вугар Фуад оглы; [Место защиты: ФГБОУ ВО «Всероссийский государственный университет юстиции (РПА Минюста России)» ; Диссовет Д 229.001.XX (10.2.002.02)]. – М., 2022. - 540 с.

Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореф. дис. ... д-ра юрид. наук: 12.00.08 / Евдокимов Константин Николаевич; [Место защиты: ФГКОУ ВО «Университет прокуратуры Российской Федерации»]. – М., 2022. – 73 с.

Карпов В. О. Культ Колумбайна: основные детерминанты массовых убийств в школах. Казань: Вестник Казанского юридического института МВД России. №4(34). 2018. С. 442 – 446.

Кирюхин В. В. Административная деятельность полиции по профилактике правонарушений несовершеннолетних: учебное пособие / В. В. Кирюхин, Н. Н. Пестов, А. С. Ускова. М.: Академия управления МВД России, 2020. 112 с.

Кочои С. М. Пробелы в законодательстве о терроризме и предложения по их устранению // Всероссийский криминологический журнал. 2016. №4. С. 740 – 749.

Макеев Н. Н. Социальные сети и подростковый суицид: проблемы реализации ч. 1 ст. 38 Конституции РФ // Конституционное и муниципальное право. 2019. № 12. С. 27 – 30.

Меняйло Д. В., Иванова Ю. А., Меняйло Л. Н. Способы профилактики и противодействия криминальному молодежному движению АУЕ. Вестник экономической безопасности, 2019. С.184 – 187.

Никитин В. В. Профилактика правонарушений в образовательных организациях в современных условиях / В. В. Никитин // Преподаватель года 2021: сборник статей II Международного профессионально-исследовательского конкурса, Петрозаводск, 14 декабря 2021 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И. И.), 2021. С. 42 – 53.

Никишин В. Д. Колумбайн (скулшутинг): сущность, правовая квалификация, криминалистическая диагностика // Lex russica. 2021. Т. 74. № 11. С. 62 – 76.

Никишин В. Д. Интернет как среда для вовлечения в экстремистско-террористические сообщества: угрозы информационно-мировоззренческой безопасности пользователей цифровой среды // Следственная деятельность: наука, образование, практика: тезисы докладов Международной научно-практической конференции (Минск, 24 июня 2021 г.) / ред. кол. С.Я. Аземша (председатель) и др. — Минск: СтройМедиаПроект, 2021. С. 56 – 60.

Никишин В. Д. Информационно-мировоззренческая безопасность личности в социальных сетях и проблемы выявления словесного экстремизма // Национальные и международные тенденции и перспективы развития судебной экспертизы: сборник докладов Всероссийской научной

конференции с международным участием, г. Нижний Новгород, 20 – 21 мая 2021 г. Нижний Новгород: ННГУ, 2021. С. 108 – 112.

Никишин В. Д. Колумбайн (скулшутинг): вопросы правовой квалификации // Вестник криминалистики, 2021. № 3 (79). С. 60 – 64.

Палий В.В. Склонение, вербовка, вовлечение как средства конструирования состава преступления // Актуальные проблемы российского права. 2023. № 12 (157). С. 114-122.

Панкова О. В. Рассмотрение в судах общей юрисдикции дел об административных правонарушениях /Панкова О. В., Егорова О. А. - Москва : Статут, 2014. - 440 с.ISBN 978-5-8354-1029-3, 1000 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/478470 (дата обращения: 13.05.2024).

Панкова, О. В. Правосудие по делам об административных правонарушениях в судах общей юрисдикции : монография / О. В. Панкова. - Москва : Статут, 2023. - 450 с. - ISBN 978-5-8354-1881-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2133916 (дата обращения: 13.05.2025)

Панфилов Е. Е. Предупреждение делинквентного поведения несовершеннолетних (на примере Тульской области) // Пробелы в российском законодательстве. 2019. № 2. С. 175 – 178.

Пономарёв С. Б., Румянцев Н. В. Сущностное содержание тюремной субкультуры и пути противодействия ее распространению: монография / С.Б. Пономарёв, Н.В. Румянцев. Белгород: ООО «Эпицентр», 2020. С. 52.

Поцелуев С. П., Подшибякина Т. А. О факторах политической радикализации в сетевой коммуникации посредством «эхокамер» // Научная мысль Кавказа. 2018. №2 (94). С. 29 – 34.

Профилактика терроризма и экстремизма в молодёжной среде. - СПб.: ООО «Издательство «Русь», 2018. 96 с.

Профилактика экстремизма и терроризма: сб. учебно- методических материалов / автор - составит: А. Г. большаков, А. М. Межведилов, Е. А. Терешина и др. Казань: Изд. Казан. Уни - та, 2012. 108 с.

Рарог А. И., Палий В. В. Уголовно-правовое противодействие терроризму и экстремизму: учебное пособие / А. И. Рарог, В. В. Палий. М.: Проспект, 2020. 96 с.

Русскевич Е. А., Чекунов И. Г. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Уголовное право. 2022. № 5. С. 26 – 35.

Русскевич Е. А. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-

телекоммуникационных сетей (ст. 274 УК РФ): вопросы квалификации // Уголовное право. – 2020. – № 5. – С. 94 – 104.

Русскевич Е. А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. № 3. С. 10 – 13.

Синицына Т. Ю., Кирюшкина А.Л. Группы смерти. Профилактика непопадания / методическое пособие. М.: Традиция, 2021. 38с.

Сичкаренко А. Ю. Ассистированное самоубийство // Законность. 2019. № 5. С. 34 – 39.

Суицидальное поведение несовершеннолетних. «Группы смерти» в социальных сетях: Методические рекомендации /Ворсина О. П., Бычкова А. М.: Иркутск, 2018. 52 с.

Устинова Т. Д. Склонение к самоубийству или содействие самоубийству: критический анализ // Lex russica. 2020. № 3. С. 151 – 159.

Хатуев В. Б. Доведение до самоубийства или до покушения на самоубийство: становление, состояние и проблемы уголовно-правовой регламентации в российском уголовном законодательстве // Актуальные проблемы российского права. 2019. № 9. С. 27 – 40.

Шиханов В. Н. Криминализация АУЕ: подводные камни реализации политико-правового решения // Сибирский юридический вестник. 2021. № 1 (92). С. 68 – 73.

Юрченко И. А. Сталкер как субъект уголовной ответственности // Вестник Университета имени О.Е. Кутафина (МГЮА). 2018. № 12. С. 53 – 61.

Юрченко И. А. Кибербезопасность как объект преступления // Судья. 2016. № 4 (64). С. 50 – 52.

3.5.4 Электронные ресурсы

Как уберечь детей от деструктивных групп в социальных сетях [Электронный ресурс]/ Сайт газеты «Калужские Губернские ведомости». 2021. 16 апреля. URL: https://kgvinfo.ru/novosti/kriminal/ne-stat-svoim-sredi-chuzhikh/ (дата обращения: 17.03.2025).

Как уберечь детей от деструктивных групп в социальных сетях [Электронный ресурс] / Сайт газеты «Калужские Губернские ведомости». 2021. 16 апреля. URL: https://kgvinfo.ru/novosti/kriminal/ne-stat-svoim-sredi-chuzhikh/ (дата обращения: 17.03.2025).

Мероприятия по профилактике деструктивного поведения подростков в условиях физкультурно-спортивной организации. Методический материал [Электронный ресурс]. URL:https://irs-krsk.ru/sites/default/files/mm_meropriyatiya_po_profilaktike_destruktivnogo_povedeniya_v_fso_2.pdf (дата обращения: 17.03.2025).

3.6. Образовательные технологии

При проведении учебных занятий по модулям образовательной программы используются традиционные и инновационные, в том числе информационные образовательные технологии, включая при необходимости применение активных и интерактивных методов обучения.

Традиционные образовательные технологии реализуются, преимущественно, в процессе лекционных и практических занятий. Инновационные образовательные технологии используются в процессе аудиторных занятий и самостоятельной работы слушателей в виде применения активных и интерактивных методов обучения.

Информационные образовательные технологии реализуются в процессе использования электронно-библиотечных систем, электронных образовательных ресурсов и элементов электронного обучения в электронной информационно-образовательной среде для активизации учебного процесса и самостоятельной работы студентов.

Самостоятельная работа слушателей подразумевает работу под руководством преподавателя (консультации) и индивидуальную работу слушателей (обучающихся), выполняемую с использованием электронных информационно-образовательных ресурсов. При реализации образовательных технологий используются следующие виды самостоятельной работы: работа с конспектом лекции (обработка текста); работа с учебниками и учебными пособиями по лекционному материалу и рекомендованной литературе; самостоятельная проработка тем и вопросов, предусмотренных программой, но не раскрытых полностью на лекциях; выполнение тестовых заданий; подготовка к практической работе; подготовка творческого задания; подготовка к аттестации.

Практические занятия относятся к интерактивным методам обучения и обладают значительными преимуществами по сравнению с традиционными методами обучения, главным недостатком которых является известная изначальная пассивность субъекта и объекта обучения.

Практические занятия могут проводиться в форме групповой дискуссии, «мозговой атаки», ролевых игр, и др. Прежде, чем дать группе информацию, важно подготовить участников, активизировать их ментальные процессы, включить их внимание, развивать кооперацию и сотрудничество при принятии решений.

Методические рекомендации по проведению различных видов практических (семинарских) занятий:

3.6.1. Обсуждение в группах

Групповое обсуждение какого-либо вопроса направлено на нахождении истины или достижение лучшего взаимопонимания, Групповые обсуждения способствуют лучшему усвоению изучаемого материала.

На первом этапе группового обсуждения перед обучающимися ставится проблема, выделяется определенное время, в течение которого обучающиеся должны подготовить аргументированный развернутый ответ.

Преподаватель может устанавливать определенные правила проведения группового обсуждения:

- задавать определенные рамки обсуждения (например, указать не менее 5…. 10 ошибок);
- ввести алгоритм выработки общего мнения (решения);
- назначить модератора (ведущего), руководящего ходом группового обсуждения.

На втором этапе группового обсуждения вырабатывается групповое решение совместно с преподавателем (арбитром).

Разновидностью группового обсуждения является круглый стол, который проводится с целью поделиться проблемами, собственным видением вопроса, познакомиться с опытом, достижениями.

3.6.2. Публичная презентация проекта

Презентация – самый эффективный способ донесения важной информации как в разговоре «один на один», так и при публичных выступлениях. Слайд-презентации с использованием мультимедийного оборудования позволяют эффективно и наглядно представить содержание изучаемого материала, выделить и проиллюстрировать сообщение, которое несет поучительную информацию, показать ее ключевые содержательные пункты. Использование интерактивных элементов позволяет усилить эффективность публичных выступлений.

3.6.3. Дискуссия

Как интерактивный метод обучения означает исследование или разбор. Образовательной дискуссией называется целенаправленное, коллективное обсуждение конкретной проблемы (ситуации), сопровождающейся обменом идеями, опытом, суждениями, мнениями в составе группы обучающихся.

Как правило, дискуссия обычно проходит три стадии: ориентация, оценка и консолидация. Последовательное рассмотрение каждой стадии позволяет выделить следующие их особенности.

Стадия ориентации предполагает адаптацию участников дискуссии к самой проблеме, друг другу, что позволяет сформулировать проблему, цели дискуссии; установить правила, регламент дискуссии.

В стадии оценки происходит выступление участников дискуссии, их ответы на возникающие вопросы, сбор максимального объема идей (знаний), предложений, пресечение преподавателем (арбитром) личных амбиций отклонений от темы дискуссии.

Стадия консолидации заключается в анализе результатов дискуссии, согласовании мнений и позиций, совместном формулировании решений и их принятии.

В зависимости от целей и задач занятия, возможно, использовать следующие виды дискуссий: классические дебаты, экспресс-дискуссия, текстовая дискуссия, проблемная дискуссия, ролевая (ситуационная) дискуссия.

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Формы текущего контроля и итоговой аттестации

Оценка качества сформированности профессиональных компетенций осуществляется в рамках текущего контроля на основе результатов тестирования, а также анализа работы обучающихся на практических занятиях.

Образовательной программой курса повышения квалификации предусмотрен итоговый контроль. Итоговый контроль является обязательным условием аттестации слушателей. Главной целью итоговой аттестации является определение сформированности профессиональных компетенций, заявленных в программе курса, также уровня знаний, умений и навыков, полученных в процессе обучения. Формой итоговой аттестации является зачет, который проводится в форме тестирования (онлайн-тестирование на платформе «Moodle» в ЭИОС КЧГУ https://do.kchgu.ru). Слушателям, успешно прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

4.2. Примеры контрольных тестовых заданий (текущий контроль)

1) Каковы основные принципы административной ответственности за правонарушения с использованием информационно-коммуникационных технологий?

а) пропорциональность;

б) справедливость;

в) конфиденциальность;

г) **все вышеперечисленное.**

Какие действия квалифицируются как нарушение правил защиты информации?

а) нарушение конфиденциальности данных;

б) несанкционированный доступ к информации;

в) распространение вредоносного ПО;

г) все вышеперечисленное.

3) Субъективная сторона преступления, предусмотренного ст. 110 УК «Доведение до самоубийства», характеризуется:

а) легкомыслием;

б) небрежностью;

в) только прямым умыслом.

4) При совершении публичных призывов к осуществлению экстремистской деятельности путем массовой рассылки сообщений абонентам мобильной связи или с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», преступление будет признаваться оконченным с момента:

а) **размещения обращений (например, на сайтах, форумах или в блогах), отправления сообщений другим лицам;**

б) когда удалось побудить других граждан к осуществлению экстремистской деятельности.

5) Обеспечение криминологической безопасности в сфере цифровых технологий рассматривается как деятельность по реализации системы (в зависимости от сферы деятельности):

а) правовых, кадровых и технических мер;

б) правовых, политических, социально-экономических, психологических и иных мер;

в) правовые и организационно-управленческих мер;

г) морально-этических, физических и технических мер.

6) Динамика мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий, в 2018—2023 гг., имеет тенденцию:

а) волнообразную;

б) снижения;

в) роста;

г) не выраженную.

7) Основные подходы к противодействию киберпреступности включают:

а) правовой и управленческий подходы;

б) **международный, правовой, технический и организационный подходы;**

в) криминологический и виктимологический подходы;

г) оперативно-разыскной и технический подходы.

Примерные вопросы к итоговому тестированию

1) Каковы сроки составления протокола об административном правонарушении в области ИКТ?

а) 24 часа после обнаружения правонарушения;

б) 2 дня после обнаружения правонарушения;

в) 10 дней после обнаружения правонарушения;

г) немедленно после выявления совершения административного правонарушения.

2) К способам склонения к самоубийству (ст. 110^1 УК РФ) не относятся:

а) угрозы;

б) уговоры;

в) обман;

г) подкуп.

3) За какие деяния наступает ответственность по ст. 282^2 УК РФ «Организация деятельности экстремистской организации»:

а) склонение;

б) вербовка;

в) участие в деятельности;

г) публичные призывы.

Критерии оценивания итоговой аттестации

Для определения уровня сформированности профессиональных компетенций слушателей разрабатываются критерии оценивания для итоговой аттестации (зачет в форме онлайн-тестирования на платформе «Moodle»). Итоговая аттестация оценивается по системе «зачтено», «не зачтено»:

- **оценка «зачтено»** выставляется, если слушатель правильно отвечает минимум на 60% вопросов;

- оценка «не зачтено» выставляется, если слушатель не набирает 60% правильных ответов на вопросы.

V. СОСТАВИТЕЛИ ПРОГРАММЫ

Тохчуков М.О. к.э.н., доцент кафедры ГМУ и политологии ФГБОУ ВО «Карачаево-Черкесский государственный университет имени У.Д. Алиева».

(подпись)

Прошито, пронумеровано и
Скреплено печатью 58 л.
_____ М.Д. Батчаева
«05» 11 2025г.