

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»**

Кафедра уголовного права и процесса

Утверждаю
Зав. кафедрой к.ю.н.,
доц. Вадампин С.К.

Протокол заседания
кафедры № 8
от «31» марта 2026 г.



Рабочая программа дисциплины

Наименование дисциплины	Профилактика НИТЕС-преступности и девиантности в киберпространстве
Направление подготовки	40.04.01 «Юриспруденция»
Профиль подготовки	Уголовное право и девиантология
Год набора	2024, 2025, 2026

Составитель

д.социол.н., профессор Ю.Ю. Комлев

Казань

Содержание

1.	Цели и задачи учебной дисциплины.....	3
2.	Место дисциплины в структуре ОПОП.....	4
3.	Требования к результатам освоения дисциплины.....	4
4.	Структура и содержание дисциплины.....	6
4.1	Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций.....	6
4.2	Содержание дисциплины по темам (разделам).....	7
4.3	Планы практических и семинарских занятий.....	10
5.	Учебно-методическое обеспечение самостоятельной работы студентов.....	13
6.	Учебно-методическое и информационное обеспечение дисциплины.....	13
7.	Материально-техническое обеспечение дисциплины.....	15
8.	Оценка компетенций по изучаемой дисциплине.....	15
Приложение 1. Методические указания для обучающихся по освоению дисциплины.....		25
Приложение 2. Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине.....		29

1.Цели и задачи учебной дисциплины

Целью дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве» является освоение студентами феноменологии высокотехнологичной преступности и девиантности в киберпространстве Интернета в современную цифровую эпоху, ее различных проявлений (интернет-зависимость, сетевая аддикция, компьютерный эскапизм, смартфон-аддикция, кибер-шопинг-аддикция, кибер-мошенничество, кибер-воровство, кибер-хулиганство, кибер-стокерство, преступность хакеров и фрикеров и др.), а также для сбора и анализа эмпирических данных о различных проявлениях киберпреступности, их диагностики для решения задач социального контроля социально-правовыми средствами путем разработки эффективных правовых основ для программы мер предупреждения правонарушений с учетом изменяющихся условий.

Задачи дисциплины:

- раскрыть многообразие и специфику форм «HIGH-TECH-девиантности» (интернет-зависимость, сетевая аддикция, компьютерный эскапизм, смартфон-аддикция, кибер-шопинг-аддикция, кибер-мошенничество, кибер-воровство, кибер-хулиганство, кибер-стокерство, преступность хакеров и фрикеров);
- описать типы кибер-девиантов и основы кибер-панк-субкультуры в мире цифровых технологий;
- на основе изучения различных форм кибердевиантности эмпирическими методами, анализа и обобщения полученных данных для их диагностики в современном цифровом обществе и решить задачи социально-правового контроля над ними в рамках девиантологических исследований;
- открывая знания о киберпреступности использовать эту информацию для разработки и осуществления программы мер по предупреждению правонарушений и преступности в сфере высоких технологий;
- изучить приемы коррекции программы мер предупреждения кибердевиантности и киберпреступности с учетом изменяющихся технологических, социально-экономических и политических условий в современном обществе.

После освоения данной дисциплины студент должен:

Знать: специфику правонарушений в киберпространстве и использовать эти знания в разработке программ их предупреждения, а также различные формы НИТЕС-преступности и девиантности и пути реализации социального контроля над ними в киберпространстве Интернета;

Уметь: применять социально-технологические знания для разработке и реализации программы мер предупреждения киберправонарушений; осуществлять программы профилактической работы, направленные на предупреждение НИТЕС-преступности и кибер-девиантности; использовать передовой отечественный и зарубежный опыт профилактической работы с учетом быстрых технологических инноваций и изменений в программах

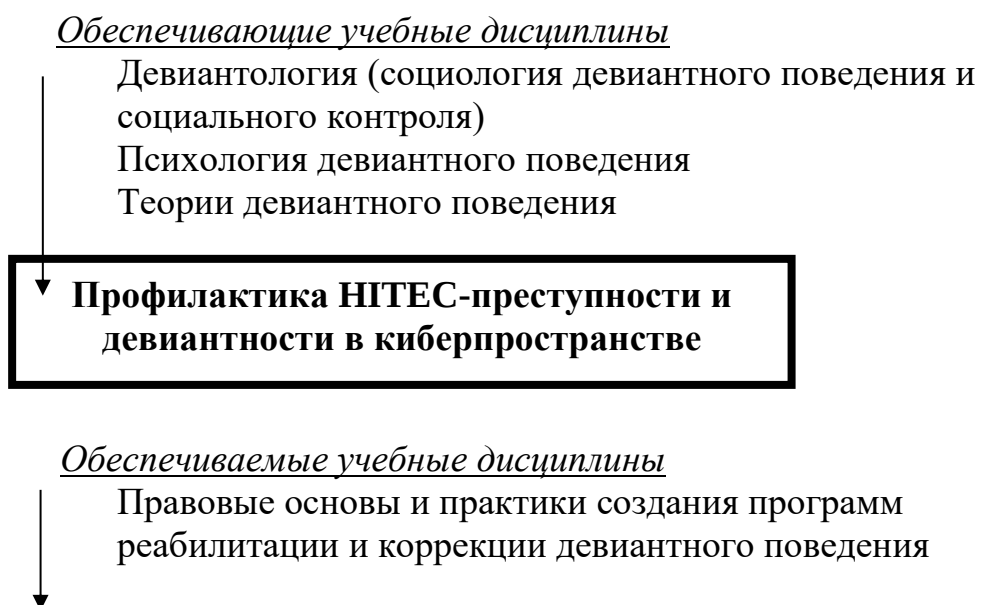
противодействия киберпреступности; использовать эмпирические методы для изучения высокотехнологичных форм девиантного поведения; анализировать и обобщать эмпирические данные для диагностики и оценки общественной опасности различных форм НИТЕС-преступности и девиантности; решать задачи социально-правового контроля над НИТЕС-преступностью и девиантностью с опорой на актуальные материалы девиантологических исследований, выполненных с учетом социально-технологических эффектов цифровизации ;

Владеть: основными практиками реализации профилактических мер над кибер-преступностью и другими проявлениями социально опасной кибер-девиантности; навыками корректировки программы мер по предупреждению высокотехнологичных правонарушений и кибердевиантности с учетом технологических инноваций; навыками эмпирического анализа различных проявлений высокотехнологичной преступности и девиантности в киберпространстве Интернета для диагностики и совершенствования мер социального контроля над ними; навыками самостоятельного решения задач социально-правового контроля над проявлениями кибер-девиантности и кибер-преступности на научной основе.

2. Место дисциплины в структуре ОПОП

Данная дисциплина относится к группе дисциплин по выбору (№ 4) части, формируемой участниками образовательных отношений. До начала изучения дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве» у студента должны быть сформированы компоненты компетенций (ЗУВы), полученные в результате изучения дисциплин по программе магистратуры: девиантология, психология девиантного поведения, теории девиантного поведения.

Дисциплина находится во взаимосвязи с дисциплинами согласно схеме:



3. Требования к результатам освоения дисциплины

Дисциплина «участвует в формировании следующих: компетенций в соответствии с ФГОС ВО по направлению «Юриспруденция» -40.04.01:

ПК-7. способен разрабатывать правовые основы и осуществлять программу мер предупреждения правонарушений, анализировать и устранять причины, препятствующие их совершенствованию

ПК-10. способен анализировать эмпирические данные для диагностики девиантности и решения задач социального контроля социально-правовыми средствами

После освоения дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве» студент должен получить следующие образовательные результаты соотнесенные с индикаторами достижения компетенций.

Декомпозиция компетенций

Индикаторы	Результаты обучения по дисциплине
Компетенция ПК-7	
ПК-7.1. Применяет знания и использует информацию для разработки программы мер по предупреждению правонарушений.	ПК-7.1. 3.2. Знает специфику правонарушений в киберпространстве и использует эти знания в разработке программ их предупреждения ПК – 7.1. У.4. Умеет применять социально-технологические знания для разработке и реализации программы мер предупреждения киберправонарушений
ПК-7.2. Осуществляет программу профилактической работы, направленную на предупреждение преступности	ПК-7.2. У.11. Умеет осуществлять программы профилактической работы, направленные на предупреждение НИТЕС-преступности и кибер-девиантности ПК – 7.2. В.7. Владеет основными практиками реализации профилактических мер над кибер-преступностью и другими проявлениями социально опасной кибер-девиантности
ПК-7.3. Учитывает изменяющиеся социально-экономические, политические условия для корректировки программы мер по предупреждению правонарушений и осуществляет ее реализацию в новых условиях	ПК-7.3. У.19. Умеет использовать передовой отечественный и зарубежный опыт профилактической работы с учетом быстрых технологических инноваций и изменений в программах противодействия киберпреступности ПК – 7.3. В.14. Владеет навыками корректировки программы мер по предупреждению высокотехнологичных правонарушений и кибердевиантностис учетом технологических инноваций
Компетенция ПК-10	
ПК-10.1. Изучает различные формы девиантности эмпирическими методами	ПК-10.1. 3.2. Знает различные формы НИТЕС-преступности и девиантности и пути реализации социального контроля над ними в киберпространстве Интернета

	ПК – 10.1. У.4. Умеет использовать эмпирические методы для изучения высокотехнологичных форм девиантного поведения
ПК-10.2. Анализирует и обобщает эмпирические данные для диагностики девиантного поведения	ПК – 10.2. У.13. Умеет анализировать и обобщать эмпирические данные для диагностики и оценки общественной опасности различных форм НИТЕС-преступности и девиантности ПК-10.2. В.11. Владеет навыками эмпирического анализа различных проявлений высокотехнологичной преступности и девиантности в киберпространстве Интернета для диагностики и совершенствования мер социального контроля над ними
ПК-10.3. Решает задачи социально-правового контроля на основе девиантологических исследований	ПК – 10.3. У.22. Умеет решать задачи социально-правового контроля над НИТЕС-преступностью и девиантностью с опорой на актуальные материалы девиантологических исследований, выполненных с учетом социально-технологических эффектов цифровизации ПК-10.3. В.20. Владеет навыками самостоятельного решения задач социально-правового контроля над проявлениями кибер-девиантности и кибер-преступности на научной основе

Этапы формирования выбранных компетенций, их индикаторов (в части ЗУВ-ов) можно проследить по Пояснительной записке и модульно-тематическому плану дисциплины.

4. Структура и содержание дисциплины

4.1. Тематический план и пояснительная записка с указанием этапов формирования компетенций

Общая трудоемкость дисциплины составляет 4/4 зачетных единиц по очному/заочному обучению (144/144 академических часа).

Наименование модулей	Количество		Самостоятельная работа	Всего часов	Индикаторы компетенций/ЗУВы
	ауд. часов				
			Очная/заочная		
<u>Модуль 1:</u> НІТЕС-преступность и девиантности в киберпространстве: феноменология и пути профилактики					
<u>Тема 2:</u> Кибер-девиантность и киберпреступность		4/2	14/12	18/14	

Наименование модулей	Количество ауд. часов		Самостоятельная работа Очная/за очная	Всего часов	Индикаторы компетенци й/ЗУВы
Тема 3: Специфика и виды киберпреступлений		4/4	14/12	18/16	ПК-7.2. У.11, В.7 ПК-7.3.
Тема 4: Кибер-субкультура и специфика НИ-ТЕСН - преступности и девиантности		4/4	14/10	18/14	У.19, В.14
Тема 5: Профилактика кибердевиантности и киберпреступности		4/4	14/10	18/14	ПК – 10.3. У.3, В.3 ПК – 10.2. У.22, В.20
Подготовка и написание курсовой работы			36/36	36/36	
Подготовка к экзамену			18/36	18/36	
ИТОГО:		20/16	124/128	144/144	

*интерактив (данная тема изучается с применением интерактивных методов обучения)

Пояснительная записка к модульному плану с этапами формирования компетенций

Данный курс состоит из одного модуля и 5-и тем.

Модуль 1 НИТЕС-преступность и девиантности в киберпространстве: феноменология и пути профилактики включает в себя 5 учебных тем.

В результате прохождения модуля студент получает представление о феноменологии киберпреступности и девиантности, способах контроля «новых девиаций в условиях 4-й технологической революции, что готовит его к профессиональной деятельности в постсовременных быстроменяющихся условиях и должен

- **Знать:** специфику правонарушений в киберпространстве и использовать эти знания в разработке программ их предупреждения, а также различные формы НИТЕС-преступности и девиантности и пути реализации социального контроля над ними в киберпространстве Интернета (ПК-7.1. 3.2, ПК-10.1.3.2)

- **Уметь:** применять социально-технологические знания для разработке и реализации программы мер предупреждения киберправонарушений; осуществлять программы профилактической работы, направленные на предупреждение НИТЕС-преступности и кибер-девиантности; использовать передовой отечественный и зарубежный опыт профилактической работы с учетом быстрых технологических инноваций и изменений в программах противодействия киберпреступности; использовать эмпирические методы для изучения высокотехнологичных форм девиантного поведения; анализировать и обобщать эмпирические данные для диагностики и оценки общественной опасности различных форм НИТЕС-преступности и девиантности; решать задачи социально-правового контроля над НИТЕС-преступностью и девиантностью с опорой на актуальные материалы девиантологических исследований, выполненных с учетом социально-технологических эффектов цифровизации (ПК – 7.1. У.4, ПК-7.2. У.11, ПК-7.3. У.19, ПК – 10.1. У.4, ПК – 10.3. У.13, ПК – 10.2. У.22)

- **Владеть:** основными практиками реализации профилактических мер над кибер-преступностью и другими проявлениями социально опасной кибер-девиантности; навыками корректировки программы мер по предупреждению высокотехнологичных правонарушений и кибердевиантности с учетом технологических инноваций; навыками эмпирического анализа различных проявлений высокотехнологичной преступности и девиантности в киберпространстве Интернета для диагностики и совершенствования мер социального контроля над ними; навыками самостоятельного решения задач социально-правового контроля над проявлениями кибер-девиантности и кибер-преступности на научной основе (ПК – 7.2. В.7, ПК – 7.3. В.14, ПК-10.2. В.11, ПК-10.3. В.20)

Уровень освоения (ПК-7, ПК-10) проверяется устным опросом, индивидуальным письменным заданием, тестом.

4.2 Содержание дисциплины по темам (разделам)

Тема1. Технологическая революция в обществе постмодерна

Количественная и качественная методология в девиантологических исследованиях высокотехнологичной преступности. Понятие «информационного общества» по терминологии И.Масуды. Понятие «общество риска» по терминологии У.Бека, характеристики и тенденции технологической революции в мире и России. Информатизация и интернетизация общества постмодерна. Понятие «виртуальной реальности» как симуляции или замещение реального мира в киберпространстве

компьютерных сетей. Понятие «социальная сеть» как интерактивный многопользовательский веб-сайт. Социальные сети как новый глобальный культурный феномен HIGH-TECH эпохи. Высокий уровень сетевой экспансии - главный тренд глобальной сети (лидеры: Facebook, микроблоговая платформа Twitter).

Тема 2. Кибер-девиантность и кибер-преступность

Кибер-девиантность: интернет-зависимость, сетевая аддикция, компьютерный эскапизм, смартфон-аддикция, кибер-шопинг-аддикция, кибер-преступность. Понятие кибер-преступности. Криминализация ряда деяний в России, связанных с правонарушениями в компьютерной сфере. Тенденции кибер-преступности. Компьютерные преступления - новая форма преступности «белых воротничков». Доходы и риски кибер-преступников. Массовые кибер-преступления как новая глобальная криминальная угроза. Технологии кибер-преступлений.

Тема 3. Специфика и виды кибер-преступлений

Виды современной кибер-девиантности и киберпреступности:

1. Кибер-мошенники. Незаконный доступ к информации как легкий путь к обогащению и недобросовестной конкуренции при использовании патентов на новые продукты, на химический состав инновационных и эффективных лекарств, на корпоративные маркетинговые стратегии и бренды, на финансовые ресурсы корпораций.

2. Кибер-воры программных продуктов. Использование несанкционированного доступа к базам данных и серверам компаний разработчиков программных продуктов и аппаратных гаджетов - еще один путь к девиантности и нелегальному обогащению. Реализация «пиратских» копий программных продуктов. Похищение конфиденциальной информации с использованием девайсов (сканеров и декодеров).

3. Кибер-хулиганы. Уничтожение или изменение приватных или конфиденциальных корпоративных данных с целью компьютерного хулиганства. Незаконное распространение компьютерных разрушительных компьютерных программ-вирусов («червей», макро- или полиморфных вирусов).

4. Хакеры. Незаконный взлом компьютерных систем. Хакерские атаки на информационные системы банков. Обнуление банковских счетов, порча содержания компьютерных серверов..

5. Кибер-сталкеры: девианты, преследующие кого-либо с использованием современных технологических средств, прежде всего, сети Интернет и сотовой связи, вызванное местью, ревностью или завистью.

6. Телефонные фриеры. Фрикинг как форма незаконного доступа к сотовому телефону.

Тема 4. Кибер-субкультура и специфика HIGH-TECH - преступности и девиантности

Атрибуты кибер-панк-субкультуры. Критерии и психологические характеристики технологичных девиантов (пионеры, кибер-хулиганы, гедонисты, вандалы, кибер-наркоманы, компьютерные «ботаники»). Специфика кибер-девиантности и кибер-преступлений: совершаются без использования насилия с помощью высокотехнологичного оборудования и имеют далеко идущие социальные последствия; последствия этих преступлений в глазах общественного мнения выглядят как менее опасные, чем деликты с применением физического насилия; преступники имеют доступ к компьютерам, информационным технологиям и технические навыки; их действия обычно связаны с манипуляцией информацией, которая прямо или косвенно создает прибыль или убытки; выделенные преступления могут быть совершены одним человеком или несколькими людьми в сговоре, в том числе с организацией; латентность.

Тема 5. Профилактика кибер-девиантности и кибер-преступности

Перспективы создания киберполиции. Использование в системах формального социального контроля новейших достижений в работе с большими данными в передаче информации, ее визуализации.

Раскрытие преступлений на основе новых технических средств получения объективной информации о виновности того или иного подозреваемого лица. Использование детекторов лжи нового поколения.

Развитие законодательства, правоохранительной и судебной системы, учитывающих новую технологическую реальность роста масштабов кибер-преступлений в обществе постмодерна.

4.3 Планы семинарских, практических и лабораторных занятий

Методические указания

Изучение курса «Профилактика ИТЕС-преступности и девиантности в киберпространстве» предполагает овладение теоретическими и практическими знаниями в области социального контроля над преступностью и другими проявлениями негативной девиантности, приобретение навыков организации социального контроля, выработку умения находить и применять теоретические решения к тем или иным конкретным социальным ситуациям.

В планах для семинарских занятий по курсу «Профилактика ИТЕС-преступности и девиантности в киберпространстве» сформулированы ключевые вопросы, подлежащие уяснению по соответствующей теме. При этом следует иметь в виду, что специальная литература по теме выбирается магистрантом по рекомендации преподавателя или самостоятельно из рекомендуемого списка, а также с учетом наличия в читальном зале или абонементе научной библиотеки «Университета управления «ТИСБИ». Кафедра обращает внимание студентов на то, что без изучения новейших учебников, другой специальной литературы, без прослушивания курсов лекций по девиантологической проблематике и их осмысления глубокое

уяснение содержания соответствующей темы невозможно либо весьма затруднено.

Сформулированные в планах занятий по соответствующей теме вопросы коллективно обсуждаются на семинарских занятиях в ходе решения соответствующей задачи либо специально (в зависимости от содержания вопроса). По мере необходимости в ходе семинарских занятий преподавателем могут формулироваться другие вопросы, которые по той или иной причине не нашли отражения в плане практического занятия.

Семинар1. Технологическая революция в обществе постмодерна

Вопросы для обсуждения

1. Количественная и качественная методология в девиантологических исследованиях высокотехнологичной преступности.
2. Понятие «информационного общества» и «общества риска» в эпоху постмодерна.
3. Характеристики и тенденции технологической революции в мире и России.
4. Понятие «виртуальной реальности» в киберпространстве компьютерных сетей.

Семинар 2. Кибер-девиантность и кибер-преступность

Вопросы для обсуждения

- 1.Содержание и соотношение понятий «кибер-девиантности» и «кибер-преступности».
- 2.Криминализация ряда форм кибердевиантности.
- 3.Состояние и тенденции кибер-преступности в мире и России.
- 4.Технологии кибер-преступлений.

Семинар3. Специфика и виды кибер-преступлений

Вопросы для обсуждения

1. Кибер-воры и кибер-мошенники: понятие и специфика.
2. Кибер-хулиганы: понятие и специфика.
3. Хакеры и фриеры:понятие и специфика.
4. Кибер-сталкеры: понятие и специфика.

Семинар №4. Кибер-субкультура и специфика HIGH-TECH - преступности и девиантности

Вопросы для обсуждения

1. Критерии, психологические характеристики и типы высокотехнологичных девиантов.
2. Атрибуты кибер-панк-субкультуры.
3. Латентность и низкая неотвратимость кибер-преступлений.

Семинар/лабораторное занятие №5. Профилактика кибер-девиантности и кибер-преступности

Вопросы для обсуждения

1. Понятие информационного социального контроля.
2. Специфика раскрытия преступлений на основе новых технических средств получения объективной информации.
3. Развитие законодательства, с учетом новой технологической реальности кибер-преступности в обществе постмодерна: отечественный и зарубежный опыт.
4. Новое в развитии правоохранительной и судебной системы с учетом четвертой технологической революции. Перспективы создания кибер-полиции.

Задания для самостоятельной работы:

1. *Выполнить анализ зарубежного опыта профилактики киберпреступности в банковской сфере.*
2. *Обосновать и разработать применительно к российским условиям компромиссную стратегию социального контроля над киберпреступностью в онлайн-банкинге.*

5. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа студентов регламентируется Положением об организации самостоятельной работы студентов.

Основными видами учебных занятий для студентов по данному курсу учебной дисциплины являются: лекции, семинарские занятия, лабораторная работа и самостоятельная работа студентов. Самостоятельная работа студентов является составной частью их учебной работы и имеет целью закрепление и углубление полученных знаний, умений и навыков, поиск и приобретение новых знаний.

Самостоятельная работа студентов включает в себя освоение теоретического материала на основе лекций, основной и дополнительной литературы; подготовку к семинарским занятиям в индивидуальном и групповом режиме. Советы по самостоятельной работе с точки зрения использования литературы, времени, глубины проработки темы и др., а также контроль за деятельностью студента осуществляется во время семинарских занятий.

Целью преподавателя является стимулирование самостоятельного, углублённого изучения материала курса, хорошо структурированное, последовательное изложение теории на лекциях, отработка навыков решения практических задач и анализа кейсов на семинарских занятиях, контроль знаний студентов.

При подготовке к семинарским занятиям и выполнении контрольных заданий студентам следует использовать литературу из приведенного в данной программе списка, а также руководствоваться указаниями и рекомендациями преподавателя.

Перед каждым семинарским занятием студент изучает план семинарского занятия с перечнем тем и вопросов, списком литературы и домашним заданием по вынесенному на семинар материалу.

Студенту рекомендуется следующая схема подготовки к семинарскому занятию и выполнению домашних заданий:

- проработать конспект лекций;
- проанализировать основную и дополнительную литературу, рекомендованную по изучаемому разделу (модулю);
- изучить решения типовых задач;
- решить заданные домашние задания;
- при затруднениях сформулировать вопросы к преподавателю.

В конце каждого семинарского занятия студенты получают «домашнее задание» для закрепления пройденного материала. Домашние задания необходимо выполнять к каждому семинарскому занятию. Сложные вопросы можно вынести на обсуждение на семинар или на индивидуальные консультации.

Для более глубокого освоения дисциплины студентам рекомендуется больше решать задач из базового учебного пособия и задачника с тестами из списка основной литературы. На семинарских занятиях приветствуется способность на основе полученных знаний находить наиболее эффективное решение поставленных проблем.

Контроль результатов в ходе СРС может быть осуществлен в результате:

- проверки конспектов;
- заслушивания докладов, обзоров, подготовленных студентами;
- рецензирования письменных работ студентов (эссе, рефератов, докладов, контрольных работ и т. д.);
- проведения контрольных работ по результатам самостоятельной работы студентов;
- проведения контрольного опроса (устно);

- рецензирования исследовательских работ;
- обсуждения с учебной группой результатов индивидуально выполненных студентами работ;
- оценки мультимедийных презентаций;
- оценки участия студента в олимпиадах, конкурсах, дискуссиях, встречах за «круглым столом».

Контроль над ходом и результатами самостоятельной работы студентов может осуществляться в сплошной, индивидуальной, выборочной формах.

В процессе самостоятельного изучения студент обязан проработать перечисленные ниже темы, для углубления теоретических знаний и практических навыков, на основании методических рекомендаций по самостоятельной работе.

Темы для самостоятельного изучения

1. Новые технологии и «новая» киберпреступность.
2. Предпосылки и реалии 4-й технологической революции
3. Компьютерный эскапизм и киберпреступность.
4. HIGH-TECH-девиантность и кибер-преступность в «новом веке»: тенденции и перспективы контроля.

6. Учебно-методическое и информационное обеспечение дисциплины

Литература:

Основная

1. Комлев Ю.Ю. Интегративная криминология. Девиантологический очерк [Электронный ресурс]: учебное пособие/ Комлев Ю.Ю.— Электрон. текстовые данные.— Казань: Казанский юридический институт МВД России, 2019.— 223 с.— Режим доступа: <http://www.iprbookshop.ru/86476.html>.— ЭБС «IPRbooks»

Дополнительная

2. Гилинский, Я. Девиантология: социология преступности, наркотизма, проституции, самоубийств и других «отклонений» : учебное пособие / Я. Гилинский. — 3-е изд. — Санкт-Петербург : Юридический центр Пресс, 2024. — 528 с. — ISBN 978-5-94201-520-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/137029.html>. — ЭБС «IPRbooks»

Интернет-ресурсы и информационные справочные системы:

1. <http://www.garant.ru/>– Система «Гарант», правовые базы российского законодательства;
2. <http://pravo.gov.ru/> Официальный интернет-портал правовой информации
3. <http://www.kodeks.ru/> Справочная правовая система Кодекс
4. <https://continent-online.com/> Информационная система континент
5. www.pravo.ru - Правовые новости;
6. www.rg.ru – сервер «Российской газеты».
7. <http://www.iprbookshop.ru> Электронно-библиотечная система «IPRbooks»
8. <https://urait.ru/> Образовательная платформа Юрайт.
9. <https://prezi.com> – Облачный сервис виртуальных презентаций.
10. <https://quizlet.com> – Интерактивные квизы и викторины
11. <https://onlinetestpad.com> – онлайн тестирование, опросы, кроссворды.

Современные профессиональные базы данных:

1. Конституционный суд РФ <https://ksrf.ru/ru>
2. Официальный сайт Президента РФ <http://www.kremlin.ru>
3. Верховный суд РФ <https://vsrf.ru/>
4. База данных «Судебные и нормативные акты РФ» <https://sudact.ru>
4. Судебная практика <http://spractic.garant.ru/> Система Гарант-
5. Законы, кодексы и нормативно-правовые акты в РФ <https://legalacts.ru/>
6. Сайт «Судебные решения» <http://судебныерешения.рф>
7. Национальная электронная библиотека <https://rusneb.ru/>
8. «Российский юридический журнал» <https://www.ruzh.org/> «Российский юридический журнал»
9. Издательская группа «Закон» <https://igzakon.ru/produce> Издательская группа «Закон»
10. Научная электронная библиотека <https://www.elibrary.ru/>
11. Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации <http://crimestat.ru/analytics>
12. «Официальный интернет-портал правовой информации» <http://pravo.gov.ru/>
13. Официальный сайт Главного информационно-аналитического центра МВД России. Статистика <https://mvd.ru/folder/101762>.
14. Персональный сайт профессора Ю.Ю.Комлева <http://www.socio-levkom-1.narod.ru/>

7. Материально-техническое обеспечение дисциплины

В процессе изучения данной дисциплины используется учебная аудитория, кабинет для самостоятельной работы студентов, читальный зал, видеопроекционное оборудование, компьютер, оснащенный типовым пакетом системного и офисного ПО, в соответствии с Реестром материально-технического обеспечения аудиторного фонда Университета управления «ТИСБИ».

В аудитории имеется компьютер с типовым пакетом системного и офисного ПО и выходом в интернет, проектор, маркерная доска-экран, звуковые колонки, комплект учебной мебели.

8. Оценка компетенций по изучаемой дисциплине

Для оценки компетентности рекомендуется использовать рейтинговую оценку знаний, умений и навыков студента по окончании изучения каждого Модуля в соответствии с Положением о модульно-рейтинговой системе организации образовательного процесс. Итоговая оценка (в баллах) складывается из баллов, набранных по каждому Модулю (семестровая оценка) и баллов, набранных, непосредственно на экзамене.

Расчет набранных баллов по дисциплине осуществляется в следующей последовательности:

$$C = \frac{K_1 + K_2 + \dots + K_n}{n} \times 0,6$$
, где К – количество баллов по модулю; n – количество модулей

$3 = K \times 0,4$, где К - количество баллов на экзамене (зачете);

$I = C + 3 + П$, где П – поощрительные баллы (от 1 до 5).

Уровень освоения компетенций	Количество баллов
компетенции не освоены	до 60 баллов
компетенции в основном освоены	от 60-70 баллов
компетенции освоены полностью	от 71 до 100 баллов

Уровень сформированности компетенций и их основные признаки

оцениваются по следующим таблицам:

Оценка уровня сформированности компетенции ПК-7
«способен разрабатывать правовые основы и осуществлять программу мер предупреждения правонарушений, анализировать и устранять причины, препятствующие их совершенствованию» в части дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве»

№ п/п	Уровни сформированности компетенции	Основные признаки уровня	Инструменты оценки сформированности уровня
1	2	3	4
1	Пороговый уровень (как минимально допустимый) (обязательный для всех студентов-выпускников вуза по завершении освоения ООП ВО) (от 60 до 70 баллов)	-Знает лишь самые простые способы разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета, и наиболее общие пути ее осуществления и коррекции с учетом изменяющихся социально-экономических, политических условий современности -Умеет лишь в целом использовать простые способы разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета, и наиболее общие пути ее осуществления и коррекции с учетом изменяющихся социально-экономических, политических условий современности -Владеет элементарными умениями и практическими навыками для разработки по шаблону правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета и наиболее общими путями ее осуществления, коррекции с учетом изменяющихся социально-экономических, политических условий современности	Устный опрос, тест, Курсовая работа Экзамен
2	Базовый уровень (относительно порогового уровня)	-Знает способы разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета, и пути ее осуществления и коррекции с учетом	Устный опрос, тест, реферат

	(От 71 до 85 баллов)	изменяющихся социально-экономических, политических условий современности -Умеет использовать способы разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета, и пути ее осуществления и коррекции с учетом изменяющихся социально-экономических, политических условий современности -Владеет умениями и практическими навыками для разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета и путями ее осуществления, коррекции с учетом изменяющихся социально-экономических, политических условий современности	Курсовая работа Экзамен
3	Повышенный уровень (относительно порогового уровня) (От 86 до 100 баллов)	-Знает основательно способы разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета, и оптимальные пути ее осуществления и коррекции с учетом изменяющихся социально-экономических, политических условий современности -Умеет в полной мере использовать способы разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета, и оптимизировать пути ее осуществления и коррекции с учетом изменяющихся социально-экономических, политических условий современности -Владеет в полной мере умениями и практическими навыками для разработки правовых основ программы мер по предупреждению правонарушений в киберпространстве Интернета и оптимальными путями ее осуществления, коррекции	Устный опрос, тест, реферат Курсовая работа Экзамен

		с учетом изменяющихся социально-экономических, политических условий современности	
--	--	--	--

Оценка сформированности компетенции ПК-10

«способен анализировать эмпирические данные для диагностики девиантности и решения задач социального контроля социально-правовыми средствами» в части дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве»

№ п/п	Уровни сформированности компетенции	Основные признаки уровня	Инструменты оценки сформированности уровня
1	2	3	4
1	Пороговый уровень (как минимально допустимый) (обязательный для всех студентов-выпускников вуза по завершении освоения ООП ВО) (от 60 до 70 баллов)	-Знает лишь наиболее простые приемы анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований -Умеет в основном использовать лишь наиболее простые приемы анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований -Владеет элементарными навыками анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований	Устный опрос, тест, Курсовая работа Экзамен
2	Базовый уровень (относительно порогового уровня) (От 71 до 85 баллов)	-Знает приемы анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований -Умеет использовать приемы анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований -Владеет навыками анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения	Устный опрос, тест, реферат Курсовая работа Экзамен

		задач социального контроля социально-правовыми средствами на основе девиантологических исследований	
3	Повышенный уровень (относительно порогового уровня) (От 86 до 100 баллов)	Знает основательно приемы анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований -Умеет в полной мере использовать приемы анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований -Владеет в полной мере навыками анализа эмпирических данных по различным формам кибердевиантности для их диагностики с целью решения задач социального контроля социально-правовыми средствами на основе девиантологических исследований	Устный опрос, тест, реферат Курсовая работа Экзамен

Приложение 1

Методические рекомендации для обучающихся по освоению дисциплины

Студентам на первом занятии необходимо ознакомиться с рабочей программой дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», где прописаны цели, задачи и трудоемкость ее изучения. Перед началом изучения дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве» необходимо повторить учебный материал обеспечивающих учебных дисциплин предшествующих курсов, которые дают основу для ее изучения.

Затем необходимо ознакомиться с порядком изучения дисциплины, т.е. модульно-тематическим планом и пояснительной запиской с указанием этапов формирования заявленных компетенций.

И, наконец, ознакомиться с порядком оценивания результатов обучения, для чего необходимо изучить следующие документы: Положение о модульно-рейтинговой системе оценивания и Принципы оценки уровня знаний, умений и навыков (характеристика ответа).

Студент должен внимательно изучить перечень основной (дополнительной) литературы и взять необходимые учебники в библиотеке.

При сдаче модулей упор делается на выявление основных факторов, их анализ и определения путей повышения экономической эффективности, полученных в результате анализа.

При подготовке к семинарскому занятию необходимо уточнить план проведения занятий, подготовить необходимую документацию. Практические занятия проводятся после лекционного изучения темы. Решение задач, приведенных в программе учебной дисциплины обязательно.

При изучении данного курса преподавателем используются интерактивные методы обучения, что помогает эффективнее сформировать заявленные компетенции. При проведении занятий с помощью интерактивных технологий группа разбивается на три команды. Каждая команда обеспечивается необходимой документацией. Занятие проводится в постоянном сравнении расчетов и выступлении участников команд.

По каждому пакету документов участники команд пишут пояснительную записку, включающую цель, основные задачи, экономический анализ ситуации, выявление резервов повышения экономической эффективности. В результате каждая из команд выносит на всеобщее обсуждение свои результаты и может быть оценена как со стороны преподавателя, так и со стороны студентов другой команды.

Интерактивные формы обучения обеспечивают высокую мотивацию, прочность знаний, творчество, коммуникабельность, командный дух, ценность индивидуальности, свободу самовыражения, акцент на деятельность, взаимоуважение и демократичность.

Изучение дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», дает не только овладение студентами знаний теории, но и приобретение навыков разрешения вопросов практического характера, выработку умения выявлять и анализировать девиантные проявления с позиций девиантологии в конкретных жизненных ситуациях, имеющих социальное значение. Первоначальным этапом приобретения таких навыков является решение специально подобранных и обработанных в учебных целях заданий и ситуаций представленных в виде задач. В планах для семинарских занятий по курсу «Профилактика НИТЕС-преступности и девиантности в киберпространстве» сформулированы узловые вопросы, подлежащие уяснению по соответствующей теме. При этом следует иметь в виду, что специальная литература по теме студентом избирается по его усмотрению, а также с учетом наличия в читальном зале или абонементе научной библиотеки «Университета управления «ТИСБИ». Кафедра обращает внимание студентов на то, что без изучения новейших учебников и другой специальной (монографической) литературы, без прослушивания курса лекций и их осмысления глубокое уяснение содержания соответствующей темы невозможно либо весьма затруднено.

Сформулированные в планах занятий по соответствующей теме вопросы коллективно обсуждаются на семинарских занятиях в ходе решения соответствующей задачи либо специально (в зависимости от содержания вопроса). По мере необходимости в ходе семинарских занятий преподавателем могут формулироваться другие вопросы, которые по той или иной причине не нашли отражения в плане семинарского занятия.

Интерактивные формы проведения занятий по курсу «Профилактика НИТЕС-преступности и девиантности в киберпространстве»

Внедрение инновационных методов в учебный процесс является на сегодня актуальной задачей. Данные методы позволяют осваивать предметы намного быстрее, максимально приближают студента к практической действительности и позволяют ему быстрее адаптироваться при работе по специальности. Учитывая эти моменты, кафедра уголовного права и процесса в обязательном порядке перевела 20% практических занятий на новые методики, включающие интерактивные технологии.

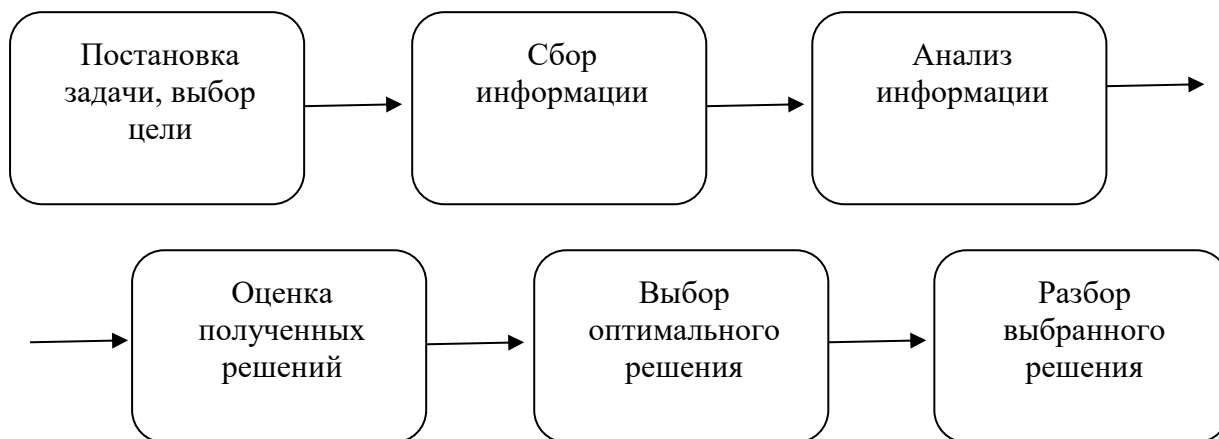
Основной упор при разработке инновационных заданий был сделан на внутрипредметные инновации, базирующиеся на построении алгоритма внедрения знаний на основе практических моделей. Это позволяет студенту применять различные способы осмысливания, обобщить усвоенный материал, применять индивидуальные склонности.

Основная методика проведения занятий построена по следующему принципу:

- студентам заранее предоставляются темы занятий и материал к самостоятельному изучению девиантологии. Перед началом занятий дается вводная 30-минутная лекция для закрепления полученных знаний и

акцентирования наиболее важных моментов. Затем студенты делятся на две группы и им предоставляется задание. Основная цель – это выступление каждой группы и взаимодополнение друг друга, с краткими выводами по полученным заданиям.

Методическая схема выполнения задания строится в следующем порядке:



При разборе выбранного решения студентами применяются эвристические приемы:

- прием аналогии - предусматривает использование подобного известного решения;
- прием инверсии – заключается в применении системы «наоборот». Прием приучает к гибкости мышления, отказу от традиционных решений, позволяет преодолевать психологическую инерцию;
- прием «мозгового штурма» - метод интенсивного генерирования новых идей путем творческого содружества группы;
- прием коллективного блокнота – позволяет сочетать независимое выдвижение идей каждым членом группы с коллективной их оценкой и процессом выработки решения;
- морфологический анализ основан на комбинаторике - систематическом исследовании всех возможных вариантов, вытекающих из анализируемого объекта.

Предложенные инновационные технологии апробированы по основным предметам кафедры: уголовное право, криминология и используются в курсе «Профилактика НИТЕС-преступности и девиантности в киберпространстве».

В результате изучения предметов с помощью инновационных технологий студенты более заинтересованы в занятиях, легче усваивают материал, быстрее запоминают.

В тоже время, при проведении занятий у преподавателей возникли определенные трудности:

- трудности, связанные с пропусками занятий. Студент, пропустивший занятие уже не может плодотворно, на одном уровне с другими, участвовать в

процессе и вынужден просто присутствовать, являясь для рабочей группы просто «балластом»;

- разный уровень усвояемости и понимания материала студентами ведет к тому, что внутри групп появляются малые группы лидеров, которые активно выполняют задания «оттесняя» остальных студентов;

- выполнение заданий требует наличие базовых знаний, полученных при ранее изученных предметах, который, к сожалению, не у всех одинаков.

Несмотря на перечисленные выше недостатки применения инновационных методов намного повышает эффективность учебного процесса и ведет к необходимости дальнейшего изучения интерактивных технологий с целью непосредственного внедрения в учебный процесс.

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»**

Кафедра уголовного права

Фонд оценочных средств
для проведения текущей и промежуточной аттестации
по дисциплине
«Профилактика НИТЕС-преступности и девиантности в
киберпространстве»
направление подготовки: Юриспруденция
профиль подготовки: Уголовное право и девиантология

Содержание

1. Паспорт фонда оценочных средств
2. Наполнение фонда оценочных средств по формам контроля
 - 2.1 Фонд оценочных средств и шкала оценивания для текущего контроля.
 - 2.1.1 Выступление на семинаре
 - 2.1.2 Тестирование
 - 2.1.3 Реферат, эссе и др. творческие работы
 - 2.2 Фонд оценочных средств и шкала оценивания для промежуточного контроля
 - 2.2.1 Фонд оценочных средств для проверки знаний и умений (вопросы к экзамену)
 - 2.2.2 Фонд оценочных средств для проверки сформированности навыков (задачи к экзамену)
 - 2.2.3 Примерная тематика и критерии оценки курсовой работы

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Формы контроля Формируемые компетенции и их индикаторы	ПК-7			ПК-10		
	ПК-7.1	ПК-7.2	ПК-7.3	ПК-10.1	ПК-10.2	ПК-10.3
Формы текущего контроля						
выступление на семинаре (устный опрос)	32			32		
тестирование письменное	У4	У11	У19	У4	У13	У22
реферат, эссе		В7	В14		В11	В20
Формы промежуточного контроля						
курсовая работа	32,У4	У11,В7	У19,В14	32,У4	У13,В11	У22, В20
экзамен	32,У4	У11,В7	У19,В14	32,У4	У13,В11	У22, В20

З- знания, У- умения, В- владения

2. Наполнение фонда оценочных средств по формам контроля

2.1. Фонд оценочных средств и шкала оценивания для текущего контроля

2.1.1 Выступление на семинаре

Выступление на семинаре является формой контроля для оценки уровня освоения компетенций, применяемой на семинарских занятиях. Выступление на семинаре может проводиться с использованием форм устного опроса, обсуждения докладов, эссе, выполненных индивидуальных заданий и проблемных вопросов.

Выступление на семинаре включает обязательную для всех магистрантов оценку текущего контроля знаний в виде устного опроса, а также выступление по проблемным вопросам спецдисциплины «Профилактика НІТЕС-преступности и девиантности в киберпространстве».

.

Примерные вопросы к семинарским занятиям

Вопросы к семинарам включают оценку закрепления материала, пройденного на лекциях, а также вопросы, направленные на выявление уровня понимания магистрантами феноменологии девиантного поведения и социального контроля.

Вопросы на проверку знаний

1. В чем специфика девиантологических исследований высокотехнологичной преступности.
2. Раскройте понятие кибердевиантности и киберпреступности.
3. В чем состоит криминализация ряда форм кибердевиантности?
4. Опишите состояние и тенденции киберпреступности в мире и России.
5. Охарактеризуйте технологии киберпреступлений и типы киберпреступников.

Критерии оценивания выступления на семинаре

Результат	Балл
Демонстрирует полное понимание поставленного вопроса, логично и последовательно отвечает на вопрос. Дает развернутый ответ с практическими примерами	100-90
Дает полный и логически правильный ответ на вопрос, но сформулировать примеры по рассматриваемому вопросу не может	80-89
Демонстрирует частичное понимание сути вопроса, способен охарактеризовать суть девиантологического феномена.	70-79
Способен сформулировать определения терминов, привести классификацию, перечислить формы, методы и т.п., но не может дать их характеристику	60-69
Демонстрирует непонимание вопроса, отвечает с наличием грубых ошибок в ответе либо не отвечает на вопросы	Менее 60

2.1.2.Тестирование

Тест на подготовку и обсуждение кейса

1.Можно ли синтезировать компромиссную модель информационного социального контроля на основе рестриктивного подхода с использованием механизма правового регулирования для любого проявления кибер-девиантности?

1. да
2. нет
3. затрудняюсь ответить

2.Если «Да», то для противодействия каким проявлениям девиантности такой синтез будет наиболее социально успешным:

1. кибер-воровство
2. кибер-хулиганство
3. кибер-терроризм
4. кибер-стокерство
5. другое _____

Опишите воображаемый кейс и предложите основные параметры рестриктивной модели на выбор из списка.

Дайте обоснованное заключение о предпочтительности вашего выбора с использованием механизма правового регулирования.

Критерии оценки уровня усвоения знаний, умений и навыков по результатам выполнения тестового задания с обсуждением кейса

Результат	Балл
Выставляется оценка «отлично» в случае правильного ответа на тестовый вопрос, а также полный развернутый ответ о применении рестриктивного подхода (кейс) для контроля кибердевиантности с описанием его основных параметров и обоснованных аргументов в пользу социальной эффективности предложенной модели;	100
Выставляется оценка «отлично» с минусом в случае правильного ответа на тестовый вопрос, а также неполный ответ о применении рестриктивного подхода (кейс) для контроля кибердевиантности с описанием его основных параметров и обоснованных аргументов в пользу социальной эффективности предложенной модели;	95
Выставляется оценка «хорошо» в случае, если дан полный, но недостаточно последовательный ответ при наличии выводов;	90
Выставляется оценка «удовлетворительно», если в ответе на тестовый вопрос отсутствуют выводы, допущены грубые ошибки;	80
Выставляется оценка «неудовлетворительно» в случае, если дан неполный и нелогичный ответ, присутствуют грубые ошибки.	от 10 до 50

2.1.3. Реферат

Реферат по проблематике кибердевиантности и киберпреступности является одним из этапов в формировании компетенций обучающегося. Реферат как форма оценочного средства предполагает краткое изложение в письменном виде содержания и результатов индивидуальной учебно-исследовательской деятельности, имеет регламентированную структуру, содержание и оформление. Его задачами являются формирование умений самостоятельной работы студентов с источниками научной литературы, их систематизация, развитие навыков логического мышления, углубление теоретических знаний по проблеме исследования.

Примерные темы рефератов

1. Методология изучения высокотехнологичной преступности.
2. Кибердевиантность в «обществе риска».
3. Состояние и тенденции технологической революции в мире и России.
4. Виртуализация социальной реальности как феномен общества постмодерна.
5. Состояние и тенденции киберпреступности в мире и России.
6. Специфику киберворовства и кибермошенничества.
7. Специфику киберхулиганства.
8. Специфика киберсталкерства.
9. Атрибуты киберпанк-субкультуры.
10. Новеллы в развитии уголовного законодательства, с учетом новой реальности кибер-преступлений.

Критериями оценки реферата являются: новизна текста, обоснованность выбора источников девиантологической литературы по вопросам высокотехнологичной преступности и девиантности в киберпространстве интернета, степень раскрытия сущности вопроса, соблюдения требований к оформлению. Новизна текста определяет, прежде всего, самостоятельностью в постановке научно-практической проблемы или формулированием нового аспекта известной проблемы, наличие авторской позиции, самостоятельность оценок и суждений.

Одним из критериев оценки работы является анализ использованной литературы. Определяется, привлечены ли наиболее известные работы по теме исследования (в т.ч. отечественные журнальные публикации последних лет, последние статистические данные, сводки, справки, зарубежные статьи и т.д.).

Степень раскрытия сущности вопроса – наиболее важный критерий оценки работы студента над рефератом. В данном случае определяется: а) соответствие плана теме реферата; б) соответствие содержания теме и плану реферата; в) обоснованность способов и методов работы с материалом, способность его систематизировать и структурировать; г) полнота и глубина знаний по теме; е) умение обобщать, делать выводы, сопоставлять различные точки зрения по одному вопросу (проблеме). Также учитывается соблюдение требований к оформлению: насколько верно оформлены ссылки на используемую литературу, список литературы; оценка грамотности и культуры изложения; владение терминологией; соблюдение требований к объёму реферата.

Критерии оценивания	Баллы
В реферате обозначена проблема в области кибердевиантности и киберпреступности, обоснована её актуальность; сделан анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция; сформулированы выводы, тема раскрыта полностью, выдержан объём; соблюдены требования к внешнему оформлению.	90-100
Основные требования к реферату выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении.	80-89
В тексте имеются существенные отступления от требований к реферированию. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании реферата; отсутствуют выводы.	66-79
Реферат представлен, но тема реферата не раскрыта, или раскрыта частично, обнаруживается существенное непонимание проблемы.	60-65

2.2 Фонд оценочных средств и шкала оценивания для промежуточного контроля

2.2.1 Фонд оценочных средств для проверки знаний и умений (вопросы к экзамену)

Вопросы к экзамену

1. Количественная методология в девиантологических исследованиях высокотехнологичной преступности.
2. Качественная методология в девиантологических исследованиях высокотехнологичной преступности.
3. Понятие «информационного общества» и «общества риска» в эпоху постмодерна.
4. Характеристики и тенденции технологической революции в мире и России.
5. Понятие «виртуальной реальности» в киберпространстве компьютерных сетей.
6. Содержание и соотношение понятий «кибер-девиантности» и «кибер-преступности».
7. Криминализация ряда форм кибердевиантности.
8. Состояние и тенденции кибер-преступности в мире и России.
9. Критерии и технологии кибер-преступлений.
10. Кибер-воры и кибер-мошенники: понятие и специфика.
11. Кибер-хулиганы: понятие и специфика.

12. Хакеры и фриеры: понятие и специфика.
13. Кибер-сталкеры: понятие и специфика.
14. Критерии, психологические характеристики высокотехнологичных девиантов.
15. Типы высокотехнологичных девиантов.
16. Атрибуты кибер-панк-субкультуры.
17. Латентность и низкая неотвратимость кибер-преступлений.
18. Понятие информационного социального контроля.
19. Специфика раскрытия преступлений на основе новых технических средств получения объективной информации.
20. Развитие уголовного законодательства, с учетом новой технологической реальности кибер-преступлений в обществе постмодерна: отечественный и зарубежный опыт.
21. Новое в развитии правоохранительной и судебной системы с учетом четвертой технологической революции.
22. Перспективы создания кибер-полиции.

2.2.2 Фонд оценочных средств для проверки сформированности навыков (задачи к экзамену)

Тестовые задачи к экзамену

1. Можно ли синтезировать компромиссную модель информационного социального контроля на основе рестриктивного подхода с использованием механизма правового регулирования для любого проявления кибер-девиантности?

1. да
2. нет
3. затрудняюсь ответить

2. Если «Да», то для противодействия каким проявлениям девиантности такой синтез будет наиболее социально успешным:

1. кибер-воровство
2. кибер-хулиганство
3. кибер-терроризм
4. кибер-стокерство
5. другое _____

Опишите воображаемый кейс и предложите основные параметры рестриктивной модели на выбор из списка.

Дайте обоснованное заключение о предпочтительности вашего выбора с использованием механизма правового регулирования.

**Критерии оценки уровня усвоения знаний, умений и навыков по
результатам экзамена по дисциплине
«Профилактика НИТЕС-преступности и девиантности в
киберпространстве»**

Характеристика ответа	Европейская оценка	Рубежные баллы	Оценка	Уровень сформированности и компетенций
Дан полный, развернутый ответ на поставленный теоретический вопрос билета на экзамене, показана совокупность осознанных знаний в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», проявляющаяся в свободном ориентировании понятиями, умении выделить существенные и несущественные его признаки, характеристики. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента. При ответе на билет на экзамене студент демонстрирует применение знаний к реальным профессиональным ситуациям и дает свою оценку решения проблемы. Причем студент не затрудняется с ответом при видоизменении задания и правильно обосновывает принятое решение, владеет характеристиками понятия и признаков социального контроля, обладает глубокими познаниями теории и механизмов социального контроля.	А	100-96	5+	Повышенный уровень сформированности компетенций
Дан полный, развернутый ответ на поставленный теоретический вопрос в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», показана совокупность осознанных знаний о предмете; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых знаний о формах, методах, тенденциях социального контроля. Знание демонстрируется на фоне понимания его места в системе данной науки и междисциплинарных связей. Умеет тесно увязывать теорию с практикой. Задача решена правильно и с обоснованием принятого решения. Ответ изложен литературным языком в терминах девиантологической науки. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.	А	95-91	5	
Дан полный, развернутый ответ на поставленный вопрос в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», доказательно раскрыты основные положения; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Задача решена верно, правильно	А	90-86	5-	

обосновывает принятую методику решения задачи. Ответ изложен литературным языком в терминах науки. В ответе допущены недочеты, исправленные студентом с помощью преподавателя.				
Дан полный, развернутый ответ на поставленный вопрос в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», показано умение выделить существенные и несущественные признаки социального контроля. Ответ четко структурирован, логичен, изложен литературным языком в терминах науки. Студент владеет разносторонними знаниями о социальном контроле, механизмах и формах его реализации. Могут быть допущены недочеты или незначительные ошибки, исправленные студентом с помощью преподавателя.	В	85-81	4+	Базовый уровень сформированности компетенций
Дан полный, развернутый ответ на поставленный вопрос в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве», показано умение выделить существенные и несущественные признаки социального контроля, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Ответы на дополнительные вопросы логичны, изложены в терминах науки, однако допущены незначительные ошибки или недочеты, исправленные студентом с помощью "наводящих" вопросов преподавателя.	С	80-76	4	
Студент демонстрирует достаточные теоретические и практические знания в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве». Дан полный, но недостаточно последовательный и исчерпывающий ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки социального контроля и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1-2 ошибки в определении основных понятий или решении практической задачи, которые студент затрудняется исправить самостоятельно.	С	75-71	4-	
Дан недостаточно полный и развернутый ответ в предметной области дисциплины «Профилактика НИТЕС-преступности и девиантности в киберпространстве». Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, касающихся основных понятий «социальный контроль», «социальный порядок». Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции. Студент испытывает затруднения при выполнении практической задачи и не может связать теорию с практикой.	D	70-66	3+	Пороговый уровень сформированности компетенций
Дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий в предметной области социального контроля над девиантностью, теорий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и	Е	65-61	3	

связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Испытывает затруднения при выполнении практических задач. Речевое оформление требует поправок, коррекции.				
Дан неполный ответ. Присутствует нелогичность изложения. Допущены существенные ошибки в основных определениях из предметной области социального контроля над девиантностью. В ответе отсутствуют выводы. Речь неграмотна. При ответе на дополнительные вопросы студент начинает понимать связь между знаниями только после подсказки преподавателя.	Е	60	3-	
Магистрант испытывает значительные трудности в ответе на вопросы. Присутствует масса существенных ошибок в определениях терминов, понятий, характеристике фактов, явлений. Речь неграмотна. На дополнительные вопросы магистрант не отвечает. Задача не решена	F	Менее 60	2	Компетенции не сформированы

2.2.3 Примерная тематика и критерии оценки курсовой работы

Примерная тематика курсовых работ

1. Количественная и качественная методология в девиантологических исследованиях высокотехнологичной преступности в «новом мире».
2. Характеристики «информационного общества» и «общества риска» в эпоху постмодерна.
3. Технологические революции и генезис преступности.
4. «Виртуализация социальной реальности и кибер-преступность.
5. Формы «кибер-девиантности» и «кибер-преступности».
6. Криминализация социально опасных форм кибер-девиантности.
7. Состояние и тенденции кибер-преступности в мире.
8. Состояние и тенденции кибер-преступности в России.
9. Технологии совершения кибер-преступлений.
10. Кибер-воры и кибер-мошенники специфика преступлений.
11. Кибер-хулиганство.
12. Хакеры и фриеры – новая социальная угроза.
13. Кибер-сталкеры: причины, проявления, следствия
14. Психологические особенности высокотехнологичных кибер-девиантов.
15. Генезис и атрибуты кибер-панк-субкультуры.
16. Понятие и пределы возможностей информационного социального контроля.

- 17.Изменения в УК с учетом новой технологической реальности кибер-преступлений (на примере зарубежного опыта).
- 18.Изменения в УК РФ с учетом новой технологической реальности кибер-преступлений.
- 19.Развитие правоохранительной и судебной системы с учетом четвертой технологической революции.
- 20.Кибер-полиция: реальность и фантомы.

Критерии оценки уровня усвоения знаний, умений и навыков по результатам написания курсовой работы

Характеристика ответа	Европейская оценка	Рубежные баллы	Оценка	Уровень сформированности компетенций
Демонстрирует глубокие знания теоретической части в предметной области дисциплин «Девиантология», «Профилактика НИТЕС-преступности и девиантности в киберпространстве» и смежных с ними социологических и юридических наук. Умеет применять полученные девиантологические знания в области анализа различных форм кибер-девиантности, стратегий и практик информационного социального контроля при практическом разрешении той или иной научно-практической проблемы с использованием механизма правового регулирования. Студент творчески подошел к написанию курсовой работы и представил свои предложения. Курсовая работа оформлена в соответствии с предъявляемыми требованиями к таким видам квалификационных работ.	A	100-96	5+	Повышенный уровень сформированности компетенций
Демонстрирует глубокие знания теоретической и практической частей курсовой работы. Умеет тесно увязывать теоретические положения девиантологии и теории информационного социального контроля с решением практических социально-коррекционных задач с помощью механизма правового регулирования. Курсовая работа оформлена в соответствии с предъявляемыми требованиями.	A	95-91	5	
Демонстрирует глубокие знания теоретической и практической частей курсовой работы. Умеет тесно увязывать теорию социального контроля с практикой. В ответах на защите курсовой работы на дополнительные вопросы допущены недочеты, исправленные студентом с помощью наводящих вопросов преподавателя. Курсовая работа оформлена в соответствии с требованиями.	A	90-86	5-	
Демонстрирует знания теоретической и практической частей курсовой работы. Студент владеет эмпирическим материалом в области анализа форм кибер-девиантности и применения стратегий и мер информационного социального контроля над тем или иным видом девиантности. Курсовая работа оформлена в соответствии с требованиями.	B	85-81	4+	Базовый уровень сформиров

Демонстрирует достаточные теоретические и практические знания. Работа выполнена без существенных ошибок в изложении материала. Ответы на дополнительные вопросы на защите работы неполные. Курсовая работа оформлена в соответствии с требованиями.	C	80-76	4	
Демонстрирует достаточные теоретические и практические знания. Работа выполнена без существенных ошибок. При устном опросе на защите работы допущены ошибки.	C	75-71	4-	
Демонстрирует определенные знания, но в работе некоторые положения не соответствуют теоретическим положениям теории социального контроля. Допущены неточности в оформлении курсовой работы.	D	70-66	3+	Порог овый уровень
Даны неполные ответы на вопросы по курсовой работе. Не все основные положения темы раскрыты. Допущены неточности в оформлении курсовой работы	E	65-61	3	
Даны неполные ответы на вопросы по курсовой работе. Присутствует нелогичность изложения. Речь неграмотна. При ответе на дополнительные вопросы на защите работы студент начинает понимать связь между знаниями только после подсказки преподавателя.	E	60	3-	
Не знает значительную часть теоретического и практического материала в предметной области социального контроля над девиантностью, допускает существенные ошибки в ответах на вопросы. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента на защите работы. Курсовая работа оформлена не в соответствии с требованиями локальных документов	F	Менее 60	2	Компетенции не сформированы