МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра уголовного права

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ О.Г. Локтионова
«27» 06 2025 г.

ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Методические указания по подготовке к практическим занятиям и выполнению самостоятельной работы для обучающихся, осваивающих ОПОП ВО – программы магистратуры, реализуемые по модели «перевернутого обучения»

Курск – 2025

УДК 343.9.01

Составитель: А.А. Гребеньков

Рецензент
Доктор юридических наук, профессор И.Б. Лагутин

Преступления в сфере высоких технологий: методические указания по подготовке к практическим занятиям и выполнению самостоятельной работы для обучающихся, осваивающих ОПОП ВО – программы магистратуры, реализуемые по модели «перевернутого обучения» / Юго-Зап. гос. ун-т; сост.: А.А. Гребеньков. – Курск, 2025. – 104 с.:– Библиогр.: с. 103-104.

Методические указания структурированы по темам дисциплины, знакомят обучающихся с алгоритмом, применяемым при реализации ОПОП ВО по модели «перевернутого обучения»; содержанием самостоятельной работы обучающихся по освоению каждой темы дисциплины и планом проведения каждого практического занятия; включают вопросы и задания, предлагаемые обучающимся для самостоятельной внеаудиторной и аудиторной работы.

Предназначены для обучающихся по очной форме обучения по ОПОП ВО – программам магистратуры, реализуемым по модели «перевернутого обучения», осваивающих дисциплину «Преступления в сфере высоких технологий».

Текст печатается в авторской редакции

Подписано в печать 28.06.25 Формат 60x84 1/16.
Усл.печ. л. 5,8. Уч.-изд. л. 5,6.
Тираж 100 экз. Заказ 837 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Освоение дисциплины «Преступления в сфере высоких технологий» в рамках ОПОП ВО – программы магистратуры, реализуемой в ФГБОУ ВО «Юго-Западный государственный университет» по модели «перевернутого обучения», имеет свои особенности, связанные со спецификой данной модели. Главная из них состоит в том, что контактная работа обучающихся с преподавателем включает в себя только практические занятия. Занятия лекционного типа по дисциплине отсутствуют.

Организовать работу по изучению каждой темы обучающемуся поможет знание алгоритма, применяемого при реализации «перевернутого обучения». Алгоритм освоения каждой темы дисциплины включает 6 последовательно совершаемых шагов или этапов, первый и второй из которых осуществляются дистанционно, остальные – очно, на практических занятиях:

1. Внеаудиторная (домашняя) самостоятельная работа студентов: предварительное (до начала первого практического занятия по теме) самостоятельное изучение обучающимися теоретического учебного контента по новой теме дисциплины.

2. Входной контроль качества освоения обучающимися основных положений темы (входной контроль знаний) в виде тестирования (проводится дистанционно до начала первого аудиторного занятия по данной теме).

3. Уточнение и (или) углубление отдельных сложных и (или) спорных вопросов на практическом занятии в рамках групповой консультации или индивидуальных консультаций.

4. Выполнение практических заданий. Работа обучающихся в малых группах по технологии ротации станций и другим технологиям.

5. Проверка практических заданий, выполненных обучающимися.

6. Текущий контроль успеваемости по изученной теме.

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться с нижеследующим описанием алгоритма, которым он будет пользоваться в дальнейшем.

1-й этап. При реализации ОПОП ВО – программы магистратуры по модели «перевернутого обучения» огромное значение приобретает первый из указанных выше этапов – этап предварительного самостоятельного освоения темы по учебно-методическим материалам, разработанным преподавателем и представленным в цифровом формате на портале **do.swsu.ru** в виде:

– инструкции для обучающегося о порядке организации самостоятельной работы по изучению данной темы, которая включает также перечень теоретических вопросов, необходимых для самостоятельного изучения;

– текста с изложением всех теоретических вопросов темы, указанных в инструкции;

– мультимедийной презентации по данной теме;

– видеоролика по данной теме.

Обучающийся имеет доступ к теоретическому учебному контенту по теме в режиме 24 / 7 и может ознакомиться с ним в любое удобное для него время в любом месте (как находясь в университете, так и за его пределами) в наиболее комфортном для него темпе, при необходимости останавливаясь в любом месте и делая паузы. Обучающийся может повторно обратиться к указанным материалам и просмотреть их неограниченное количество раз. Также обучающийся может пользоваться данными материалами непосредственно на практическом занятии.

Цель обучающегося на первом этапе – понять и запомнить теоретический учебный материал по изучаемой теме.

В начале работы по изучению теоретического учебного контента по новой теме необходимо прочитать инструкцию преподавателя. В инструкции приводится перечень теоретических вопросов, которые должен изучить обучающийся по конкретной теме, и предлагается порядок организации самостоятельной работы обучающегося по изучению данной темы. Перечисленные вопросы являются обязательными для изучения. Заданного в инструкции порядка организации самостоятельной работы рекомендуется придерживаться, но обучающийся имеет право адаптировать данный порядок для себя.

Подробно конспектировать изученный теоретический материал не требуется, но при работе с текстом для лучшего запоминания и усвоения учебной информации обучающимся предлагается фиксировать термины, основные теоретические положения, записывать ключевые слова в виде опорного конспекта или ментальной карты (интеллект-карты). (Ментальная карта (от англ. «mind map») – современный и распространенный в мире метод визуального представления идей, задач, концепций и любой другой информации**.** Это схема визуального представления информации, которая отражает взаимосвязь между несколькими элементами. Структура карты внешне напоминает дерево: в центре располагают основную идею, тему, проблему, ключевое слово, вопрос и т.п., а от нее (него) в разные стороны разводят «ветви» (стрелки), каждая из которых визуализирует связанные с главной (главным) термины, наименования, аргументы, примеры, выводы и др.)).

После тщательного изучения материалов, представленных преподавателем, обучающийся может продолжить работу над темой по источникам, указанным в разделах 8-9, 11 рабочей программы дисциплины. Самостоятельная работа с дополнительной литературой (учебной, справочной, научной), материалами периодических изданий и Интернета способствует более глубокому усвоению изучаемого материала. При работе с источниками и литературой необходимо:

– сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;

– обобщать полученную информацию, оценивать прочитанное;

– фиксировать основное содержание прочитанного текста; формулировать устно и письменно основную идею текста; составлять план, формулировать тезисы.

По завершении самостоятельного изучения темы целесообразно в качестве самоконтроля вслух пересказать положения, указанные преподавателем в инструкции как вопросы, обязательные для изучения. Необходимо добиться глубокого, осознанного освоения содержания темы и свободного владения им, в том числе терминологией.

2-й этап. После изучения темы обучающийся выполняет входное тестирование (не является формой текущего контроля успеваемости, но является обязательным). В одном варианте входного тестирования, как правило, 25 вопросов во всех 4 формах, представленных в подразделе 7.3.1 рабочей программы дисциплины. Входное тестирование оценивается по дихотомической шкале: «прошел входное тестирование» / «не прошел входное тестирование». При получении отрицательной оценки необходимо еще раз перечитать и просмотреть все теоретические учебные материалы, представленные преподавателем в цифровом формате, и пройти входное тестирование повторно до получения положительного результата.

3-й этап. По результатам самостоятельной работы и входного тестирования обучающийся определяет непонятные, и (или) сложные для него, и (или) спорные вопросы; преподаватель со своей стороны также по результатам входного тестирования устанавливает вопросы, которые необходимо уточнить и (или) углубить на практическом занятия для всей группы или для нескольких конкретных студентов. Данные вопросы могут быть рассмотрены концентрированно в начале занятия или постепенно в ходе всего занятия в рамках групповой консультации или индивидуальных консультаций (в зависимости от количества обучающихся, нуждающихся в дополнительных пояснениях преподавателя в каждом конкретном случае). Индивидуальная работа с каждым обучающимся поможет оперативно ликвидировать пробелы в его знаниях.

4-й этап является главным и самым продолжительным этапом практического занятия. Работа обучающихся на данном этапе, как правило, организуется в малых группах (3-5 человек) по технологии ротации станций, но также может организовываться и по иным технологиям.

При реализации технологии ротации станций пространство аудитории условно или буквально делится на несколько станций, количество которых совпадает с количеством малых групп.

На одной из станций группа работает с преподавателем, на других – самостоятельно. На всех остальных станциях группа выполняет одно общее практическое задание или все члены группы выполняют индивидуальные, но однотипные, похожие практические задания.

Задания на станциях направлены на формирование у обучающихся когнитивных умений и навыков всех уровней, начиная с низкого до высокого в приведенном ниже порядке:

– понимание основных положений данной темы;

– применение полученных самостоятельно знаний в конкретной производственной ситуации;

– анализ и синтез информации или каких-либо данных;

– оценку информации, данных, объектов, субъектов и т.д.;

– создание нового на основе полученных знаний, умений и навыков.

На всех станциях имеются необходимые для выполнения задания материалы (учебная, учебно-методическая и (или) научная литература; нормативные акты; инструкции, памятки и т.д.).

Время работы групп на одной станции строго ограничено, одинаково для всех станций и устанавливается преподавателем: 10, 15, 20, 25 минут или иное. По наступлении дедлайна группы по часовой стрелке переходят на следующую станцию и выполняют практическое задание этой станции.

Таким образом, в течение практического занятия каждая группа проходит все станции, в том числе ту, на которой устно отвечает на вопросы преподавателя. Преподаватель, общаясь поочередно со всеми группами, определяет уровень освоения и понимания темы каждым студентом, и дает необходимые индивидуальные консультации. Каждая группа, поработав на всех станциях, выполняет полный пакет практических заданий, подготовленных преподавателем для данного практическогозанятия.

5-й этап. В самом конце практического занятия озвучиваются и коллективно обсуждаются решения всех практических заданий. Группы выступают поочередно: каждая предлагает свое решение задания той станции, на которой в данный момент находится, в обсуждении которого участвуют все остальные группы.

6-й этап. Текущий контроль успеваемости по изученной теме осуществляется, как правило, в конце последнего практического занятия по данной теме или постфактум дистанционно. Формы текущего контроля успеваемости указаны в таблице 4.1.2 рабочей программы дисциплины; в полнотекстовом виде оценочные средства приведены в оценочных средствах для текущего контроля знаний и промежуточной аттестации обучающихся по дисциплине «Преступления в сфере высоких технологий».

При подготовке к промежуточной аттестации по дисциплине необходимо повторить основные теоретические положения каждой изученной темы и основные термины, самостоятельно решить несколько типовых

компетентностно-ориентированных задач. Доступ обучающихся к теоретическому учебному контенту, представленному в цифровом формате, дедлайнами не ограничен и возможен как при подготовке к промежуточной аттестации по дисциплине, так и в течение всего периода освоения ими ОПОП ВО, реализуемой по модели «перевернутого обучения».

ТЕМА № 2
ПОНЯТИЕ И ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

I. ДИСТАНЦИОННАЯ ЧАСТЬ

Задания, выполняемые до начала первого практического занятия по теме № 2

1. Внеаудиторная (домашняя) самостоятельная работа обучающихся по освоению основных положений темы № 2: предварительное (до начала первого практического занятия по теме) самостоятельное изучение теоретического учебного контента по новой теме дисциплины, разработанного преподавателем и представленного в цифровом формате на портале do.swsu.ru

1.1 Ознакомьтесь с **инструкцией** о порядке организации самостоятельной работы по изучению данной темы и следуйте ей.

1.2. Прочитайте **перечень основных теоретических вопросов**, которые необходимо самостоятельно освоить, и **текст с изложением указанных вопросов**.

1.3 Работая с текстом, вносите по мере чтения необходимые записи в **опорный конспект**, который поможет вам запомнить главное.

Опорный конспект по теме № 2 «Понятие и общая характеристика преступлений в сфере высоких технологий. Компьютерные преступления»

1. ЗАПОМИНАЕМ ГЛАВНОЕ

1.1. **Впишите пропущенные слова/даты:**

а) История преступности, использующей информационные технологии, насчитывает чуть более _____ лет.

б) Серийный выпуск ЭВМ, находящихся в свободной продаже, начался в _____-х годах.

в) Первые преступления с использованием ЭВМ зафиксированы в конце _____-х – _____-х годах.

г) В СССР хищение с использованием компьютера впервые зарегистрировано в _____ году в г. _____.

д) Появление глобальных компьютерных сетей (ARPAnet, Internet и др.) относится к _____-м годам.

е) КИБЕРВЫМОГАТЕЛЬСТВО – это _____ первые случаи которого зафиксированы в конце _____-х годов.

1.2. **Дайте определения ключевым понятиям:**

а) ИНФОРМАЦИОННЫЕ ПРЕСТУПЛЕНИЯ – это запрещённые уголовным законодательством под угрозой наказания виновно совершённые общественно опасные деяния, механизм совершения которых предполагает использование _____ и (или) _____.

б) ИНФОРМАЦИОННАЯ ПРЕСТУПНОСТЬ – это негативное, исторически изменчивое социально-правовое явление, представляющее собой систему _____, механизм совершения которых предполагает использование _____ и (или) _____.
Отличительная черта: практически лишена _____ локализации.

в) КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ (согласно примечанию к ст. 272 УК РФ) – это сведения (сообщения, данные), представленные в форме _____, независимо от средств их _____, _____ и _____.

г) ВРЕДОНОСНАЯ КОМПЬЮТЕРНАЯ ПРОГРАММА – это программа, предназначенная для неправомерного _____, _____, _____, _____ информации, нарушения работы ЭВМ, системы ЭВМ или их сети, а также _____.

1.3. **Перечислите основные угрозы в сфере высоких технологий (не менее 5):**

1. _____
2. _____
3. _____
4. _____
5. _____ ...

2. СИСТЕМАТИЗИРУЕМ КЛЮЧЕВЫЕ ПОНЯТИЯ И КЛАССИФИКАЦИИ

2.1. **Заполните таблицу «Группы информационных преступлений»:**

№	Группа преступлений	Краткая характеристика и пример
1	Специфически информационные преступления	Деяния, совершаемые только с использованием ИТ и/или ИТС. Пример:
2	Преступления общеуголовного характера, где ИТ/ИТС	_____. Пример: _____
3	Преступления общеуголовного характера, где ИТ/ИТС	_____. Пример: _____

2.2. **Укажите компоненты информационной безопасности и кратко раскройте их суть:**

а) КОНФИДЕНЦИАЛЬНОСТЬ – _____ .

б) ЦЕЛОСТНОСТЬ – _____ .

в) ДОСТУПНОСТЬ – _____ .

2.3. **Модель «Как услуга» («as a service») в криминальной сфере. Впишите пропущенные типы сервисов:** Основная особенность модели: выделение обособленной группы решений, направленных на удовлетворение _____ потребности, и оформление её как целостного продукта, доступ к которому предоставляется с использованием _____ сетей на основе _____ технологий. Типы криминальных сервисов:

1. Вредоносное ПО как услуга (MaaS)
2. _____ как услуга 3. _____ как услуга

3. АНАЛИЗ ОТДЕЛЬНЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ (Глава 28 УК РФ)

3.1. **Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.** а) Объект: общественные отношения в сфере безопасности _____. б) Предмет: _____ информация. в) Объективная сторона характеризуется: * Деянием в форме _____ доступа к охраняемой законом компьютерной информации. * Обязательными последствиями (хотя бы одно): _____, _____, _____, _____ компьютерной информации. * Причинной связью между _____ и _____. г) Состав по конструкции (материальный/формальный): _____. д) Субъективная сторона: вина в форме _____ по отношению к деянию (доступу) и _____ по отношению к последствиям. е) Субъект: общий – физическое вменяемое лицо, достигшее ____ лет. Специальный субъект (ч.3) – лицо, использующее свое _____.

3.2. **Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ.** а) Предмет преступления: _____. б) Альтернативные деяния объективной стороны: * _____ вредоносных программ; * Внесение изменений в _____; * _____ вредоносных программ; * _____ вредоносных программ или машинных носителей с ними. в) Субъективная сторона: прямой _____. Лицо осознает, что программа является _____ и желает совершить указанные действия. г) Квалифицирующий признак (ч.2) – совершение деяния группой лиц по предварительному сговору или _____, или _____. д) Особо квалифицирующий признак (ч.3) – если деяния повлекли _____.

3.3. **Статья 274.1 УК РФ. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.** а) Объекты посягательства: информационные системы, ИТС, АСУ, функционирующие в сферах: _____, науки, _____, связи, _____, банковской сфере и иных сферах финансового рынка, _____ комплекса, в области атомной энергии, _____, ракетно-космической, _____, металлургической и _____ промышленности. б) Обязательное условие для признания объекта КИИ предметом данного преступления: объекту должна быть присвоена _____ и он должен быть включен в _____ значимых объектов КИИ. в) Проблемный аспект: Реестр значимых объектов КИИ является _____, что затрудняет доказывание _____ вины.

3.4. **Статья 274.2 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации… (новая редакция – нарушение правил эксплуатации технических средств противодействия угрозам).** а) Данный состав является _____ -преюдициальным. б) Субъект преступления (специальный): _____ лицо или _____ _____. в) Для привлечения к уголовной ответственности по данной статье необходимо, чтобы лицо ранее было подвергнуто _____ _____ за аналогичное правонарушение (указать статьи КоАП РФ, если помните: ч.1 ст. 274.2 УК РФ – ст. _____ КоАП РФ; ч.2 ст. 274.2 УК РФ – ст. _____ КоАП РФ).

4. ПРОБЛЕМНЫЕ ВОПРОСЫ И АСПЕКТЫ ДЛЯ ОБСУЖДЕНИЯ

4.1. Сформулируйте не менее двух спорных вопросов, связанных с квалификацией компьютерных преступлений, исходя из материала лекции:

1.

_____

_____

2.

_____

_____

4.2. В чем заключаются основные недостатки легального определения «компьютерной информации», данного в примечании к ст. 272 УК РФ?

_____

_____

_____

5. РЕФЛЕКСИЯ

Сформулируйте кратко вывод, который Вы сделали лично для себя после изучения данной темы: ВЫВОД ЛИЧНО ДЛЯ СЕБЯ:

1.4 Посмотрите **видеоролик** по теме № 2 в ходе чтения текста (параллельно с ним).

Обратите внимание на то, что, несмотря на неудачную формулировку в статье 272 УК РФ, под компьютерной информацией следует понимать сведения, содержащиеся и (или) обрабатываемые в информационных системах, передаваемые по информационно-телекоммуникационным сетям, либо зафиксированные на материальных носителях, предназначенных для обработки в информационных системах, а также выраженные в форме последовательности команд для автоматического исполнения информационные технологии, с помощью которых обрабатывается информация в информационных системах и обеспечивается функционирование данных информационных систем.

1.5 Перескажите изученный теоретический материал по вопросам, указанным в инструкции, и опорному конспекту. Воспользуйтесь также следующими **вопросами для самоконтроля**:

1. Как давно появились первые преступления, совершаемые с использованием информационных технологий?
2. Какие факторы способствовали возникновению и распространению компьютерных преступлений в 1980-х годах?

3. Приведите примеры основных угроз в сфере высоких технологий, актуальных на сегодняшний день.
4. В чем заключается суть модели "как услуга" ("as a service") в высокотехнологичных отраслях экономики? Приведите примеры.
5. Дайте определение информационным преступлениям.
6. Какие две основные группы информационных преступлений выделяются по способу их совершения? Приведите примеры для каждой группы.
7. В чем заключается отличие информационной преступности от других видов преступности с точки зрения пространственной локализации?
8. Какие положительные стороны может иметь информационная преступность?
9. Как Норберт Винер определял понятие "информация"? В чем особенность информации, отличающая ее от материи и энергии?
10. Что понимается под "компьютерной информацией" в международных документах?
11. Какое определение компьютерной информации дано в Уголовном кодексе РФ? В чем заключаются недостатки этого определения?
12. Что является родовым и видовым объектом преступлений в сфере компьютерной информации?
13. Перечислите возможные последствия неправомерного доступа к компьютерной информации, предусмотренные ст. 272 УК РФ.
14. В чем заключаются особенности субъективной стороны преступления, предусмотренного ст. 272 УК РФ?
15. В чем особенности квалификации преступлений, предусмотренных ст. 272.1 УК РФ?
16. Что такое вредоносная программа? Какие действия с вредоносными программами образуют состав преступления, предусмотренный ст. 273 УК РФ?
17. Что такое критическая информационная инфраструктура Российской Федерации?
18. В чем особенности субъекта преступления, предусмотренного ст. 274.2 УК РФ?
19. Что такое административная преюдиция и в чем ее значение для ст. 274.2 УК РФ?
20. В чем состоят основные проблемы доказывания по делам о преступлениях в сфере компьютерной информации?

1.6 Возьмите с собой на практическое занятие свой **опорный конспект** по теме № 2.

1.7 Выполните **входное тестирование** по теме № 2.

Ответьте на вопросы и выполните задания в тестовой форме по теме № 2:

Вопросы в закрытой форме:

1. Укажите, в каком году на территории СССР было впервые зарегистрировано хищение денежных средств с использованием компьютера: а) 1969 г. б) 1970 г. в) 1979 г. г) 1983 г. д) 1950 г.
2. Какое из перечисленных явлений НЕ относится к основным угрозам в сфере высоких технологий, упомянутым в лекционном материале? а) Использование вредоносных программ для создания «ботнетов». б) Атаки типа Denial of Service (DoS). с) Использование компьютерной техники для планирования террористических операций. г) Естественный износ аппаратного обеспечения компьютерных систем. д) Создание распределённых сетей обмена информацией, нарушающей авторские права.
3. Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации», информация – это: а) Программы, способные обязать компьютерную систему выполнять ту или иную функцию. б) Сведения (сообщения, данные) независимо от формы их представления. в) Информация, находящаяся в памяти компьютера, на машинных или иных носителях. г) Сведения (сообщения, данные), представленные в форме электрических сигналов. д) Данные, которые не передаются на исполнение, а лишь хранятся и преобразуются.
4. Какое из перечисленных последствий неправомерного доступа к компьютерной информации (ст. 272 УК РФ) означает приведение ее в непригодное для использования состояние без возможности восстановления? а) Блокирование информации. б) Модификация информации. в) Копирование информации. г) Уничтожение информации. д) Шифрование информации.
5. В соответствии со ст. 272.1 УК РФ, к специальным категориям персональных данных, незаконный оборот которых влечет более строгую ответственность, НЕ относятся: а) Данные несовершеннолетних. б) Биометрические данные. в) Данные о политических взглядах. г) Данные о месте работы лица. д) Данные о состоянии здоровья.
6. Какое действие с вредоносными программами, согласно ст. 273 УК РФ, означает предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами? а) Создание. б) Внесение изменений. в) Использование. г) Распространение. д) Тестирование.
7. Какой квалифицирующий признак НЕ указан в ч. 2 ст. 272 УК РФ (Неправомерный доступ к компьютерной информации)? а) Причинение крупного ущерба. б) Совершение деяния из корыстной заинтересованности. в) Совершение деяния группой лиц по предварительному сговору. г) Совершение деяния с использованием

своего служебного положения. д) Все перечисленные признаки указаны в ч. 2 ст. 272 УК РФ.

8. Субъектами критической информационной инфраструктуры (КИИ) в соответствии с ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" могут быть: а) Только государственные органы и учреждения. б) Только российские юридические лица. в) Только индивидуальные предприниматели. г) Государственные органы, учреждения, российские юридические лица и индивидуальные предприниматели, владеющие определенными информационными системами. д) Любые физические лица, использующие интернет.
9. Для привлечения к уголовной ответственности по ст. 274.2 УК РФ (Нарушение правил эксплуатации технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ сети "Интернет" и сети связи общего пользования) обязательным условием является: а) Наступление тяжких последствий. б) Совершение преступления организованной группой. в) Предварительное привлечение лица к административной ответственности за аналогичное правонарушение. г) Использование своего служебного положения. д) Наличие корыстной заинтересованности.
10. Какое из определений «компьютерной информации» содержится в Конвенции о преступности в сфере компьютерной информации? а) Сведения (сообщения, данные), представленные в форме электрических сигналов. б) Любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы. в) Информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ. г) Последовательность команд, которые исполняются аппаратным обеспечением компьютера. д) Сведения, зафиксированные на материальных носителях, предназначенных для обработки в информационных системах.
11. Какой из перечисленных видов сервисов "as a service" предполагает предоставление заказчику управления над большим числом контролируемых преступниками информационных систем? а) Вредоносное ПО как услуга. б) DDoS-атаки как услуга. в) Ботнет как услуга. г) Фишинг как услуга. д) Спам как услуга.
12. Родовым объектом преступлений в сфере компьютерной информации, согласно представленному материалу, являются: а) Информационная безопасность. б) Общественная безопасность и общественный порядок. в) Конституционные права и свободы человека и гражданина. г) Экономическая безопасность государства. д) Отношения в сфере интеллектуальной собственности.

Вопросы в открытой форме:

13. Преступления, которые могут быть совершены только с использованием информационных технологий и (или) ИТС, например, компьютерные преступления или компьютерное мошенничество, относятся к группе _____ информационных преступлений.
14. Состояние защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства, называется _____.
15. Согласно определению, данному в УК РФ (ст. 272), под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме _____, независимо от средств их хранения, обработки и передачи.
16. Представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определённого результата, включая подготовительные материалы и порождаемые ею аудиовизуальные отображения, – это _____.
17. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, квалифицируется по статье _____ УК РФ.
18. Модель организации производственно-технических процессов, при которой определённая обособленная группа связанных между собой технических и организационных решений оформляется как целостный продукт, доступ к которому предоставляется с использованием ИТС на основе «облачных» технологий, условно обозначается словосочетанием «_____».

Вопросы на установление правильной последовательности:

19. Расположите в хронологическом порядке следующие события в истории компьютерных преступлений, начиная с самого раннего:
    1. Серийный выпуск ЭВМ, находящихся в свободной продаже.
    2. Регистрация хищения денежных средств с использованием компьютера на территории СССР в Вильнюсе.
    3. Совершение Альфонсом Конфессоре налогового преступления с незаконным доступом к информации в компьютерной сети.
    4. Остановка главного сборочного конвейера «АвтоВАЗа» с помощью «логической бомбы».
20. Расположите компоненты информационной безопасности в порядке, соответствующем их общепринятому перечислению (CIA Triad):
    1. Доступность

2. Целостность
3. Конфиденциальность

Вопросы на установление соответствия:

21. Установите соответствие между угрозой в сфере высоких технологий и ее описанием: А) Использование вредоносных программ для создания «ботнетов» Б) Атаки типа DDoS В) Использование средств ведения «информационной войны» Г) Создание распределённых («пиринговых») сетей обмена информацией
    1. Перегрузка целевого компьютера запросами для блокировки доступа легальных пользователей.
    2. Установление контроля над большим числом компьютеров для незаконных действий.
    3. Хранение и распространение информации (нарушающей авторские права, порнографической и иной) тысячами пользователей без единого центра.
    4. От информационной блокады до проведения диверсий на стратегических объектах на межгосударственном уровне.
22. Установите соответствие между статьей УК РФ и основным содержанием ее диспозиции: А) Ст. 272 УК РФ Б) Ст. 273 УК РФ В) Ст. 274.1 УК РФ Г) Ст. 272.1 УК РФ
    1. Создание, использование и распространение вредоносных компьютерных программ.
    2. Неправомерный доступ к компьютерной информации.
    3. Незаконные действия с персональными данными, содержащимися в компьютерной информации.
    4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
23. Установите соответствие между группой информационных преступлений и ее характеристикой: А) Специфически информационные преступления Б) Преступления общеуголовного характера, где ИТ существенно облегчают совершение В) Преступления общеуголовного характера, где ИТ не оказывают значительного влияния
    1. Развратные действия, совершенные через Интернет, воздействующие на значительное число малолетних.
    2. Обмен сообщениями по сети Интернет между соучастниками при планировании убийства.
    3. Неправомерный доступ к компьютерной информации.
24. Установите соответствие между понятием, связанным с компьютерной информацией, и его определением: А) Программа для ЭВМ Б) Данные В) Компьютерная информация (согласно Соглашению СНГ) Г) Информационные технологии

1. Информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающуюся по каналам связи.
2. Последовательность команд, которые исполняются аппаратным обеспечением компьютера.
3. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
4. Информация, которая не передается на исполнение, а лишь хранится и преобразуется в компьютерной системе.

25. Установите соответствие между квалифицирующим признаком по ст. 272.1 УК РФ (Незаконные сбор, хранение, использование или распространение персональных данных) и его содержанием: А) Корыстная заинтересованность Б) Крупный ущерб В) Трансграничная передача информации Г) Использование служебного положения
    1. Передача персональных данных за пределы территории РФ.
    2. Злоупотребление должностными полномочиями или доступом к информационным системам.
    3. Ущерб на сумму, превышающую 1 миллион рублей.
    4. Стремление к получению материальной выгоды.

II. АУДИТОРНАЯ ЧАСТЬ

Практическое занятие № 2

«Понятие и общая характеристика преступлений в сфере высоких технологий. Компьютерные преступления»

Цель практического занятия – приобретение обучающимися практического опыта в применении знаний, полученных при самостоятельном освоении темы № 2, в производственных ситуациях.

Планируемые результаты обучения:

Знать:	**Уметь:**	**Иметь опыт деятельности:**
содержание норм, устанавливающих ответственность за преступные деяния, связанные с преступлениями в сфере высоких технологий,	использовать информацию о нормах, устанавливающих ответственность за преступления в сфере высоких технологий, в целях их реализации; применять нормы особенной части	по обобщению и анализу информации, имеющей значение для реализации правовых норм в сфере установления ответственности за преступления в сфере высоких технологий;

особенности их реализации; методологические основы реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; содержание постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, связанных с уголовно-правовым регулированием ответственности за преступления в сфере высоких технологий; особенности оценки на соответствие признакам преступления (квалификации) конкретных преступлений в сфере высоких технологий, предусмотренных уголовным законодательством; способы толкования норм уголовного законодательства, позволяющие вычленить из их текста основные юридически

уголовного права, регулирующие ответственность за преступления в сфере высоких технологий; применять нормы особенной части уголовного права, регулирующие ответственность за преступления в сфере высоких технологий с учётом постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований; давать полную и точную квалификацию преступлений в сфере высоких технологий, с учётом положений Общей и Особенной части уголовного законодательства, разъяснений Пленума Верховного Суда РФ; толковать положения актов уголовного законодательства, касающиеся высоких технологий, основываясь на общих принципах толкования нормативных актов; разъяснять содержание норм уголовного законодательства, предусматривающих

по реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по обобщению и анализу постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, касающихся норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по принятию решений, связанных с оценкой на соответствие конкретных деяний, связанных с высокими технологиями, признакам преступления; по применению основных подходов к толкованию норм уголовного законодательства Российской Федерации, касающихся высоких технологий, и

значимые признаки преступных деяний, связанных с высокими технологиями, и сопоставить их с признаками преступления; особенности толкования норм уголовного законодательства, устанавливающих ответственность за конкретные преступления в сфере высоких технологий, позволяющие разграничить между собой смежные составы преступлений при наличии конкуренции норм	ответственность за совершение конкретных преступлений в сфере высоких технологий, с учётом судебной практики и доктрины уголовного права; устанавливать содержание оценочных признаков норм уголовного законодательства, регулирующих ответственность за преступления в сфере высоких технологий, а также признаков, позволяющих разграничить между собой смежные преступные деяния при наличии конкуренции норм	вычленению признаков конкретного деяния; по выявлению точного содержания норм уголовного законодательства, устанавливающих общие условия уголовной ответственности и освобождения от неё, а также признаки конкретных составов преступлений, связанных с преступлениями в сфере высоких технологий; по применению приёмов научного мышления, позволяющих устанавливать смысл нормоустановлений уголовно-правового характера, касающихся высоких технологий, в условиях правовой неопределённости, коллизий правового регулирования, конкуренции норм

Необходимое материально–техническое оборудование: ноутбук и (или) мобильные устройства преподавателя и обучающихся.

ПЛАН ПРАКТИЧЕСКОГО ЗАНЯТИЯ № 2

1. Уточнение и (или) углубление отдельных вопросов по теме № 2.
2. Выполнение обучающимися практических заданий.
3. Проверка практических заданий, выполненных обучающимися.
4. Текущий контроль успеваемости по теме № 2

1. Уточнение и (или) углубление отдельных вопросов по теме № 2
Консультация преподавателя

Студенты методом мозгового штурма формируют перечень вопросов, которые при самостоятельном освоении темы дома или при тестировании остались для них непонятными или показались сложными и (или) спорными. Преподаватель по результатам тестирования при необходимости добавляет в сформированный обучающимися список вопросы, которые, с его точки зрения, требуется уточнить или углубить.

Определяя с помощью поднятых рук количество студентов, считающих сложным конкретный вопрос из сформированного списка, преподаватель устанавливает вопросы, по которым сразу же проводит групповую консультацию.

Если в пояснениях нуждаются 1-2 человека, преподаватель индивидуально консультирует их в ходе практического занятия.

2. Выполнение обучающимися практических заданий

На данном практическом занятии выполнение обучающимися практических заданий проводится по технологии проблемного обучения с элементами проектной деятельности и кейс-метода.

Аудиторное занятие 1: Понятие и общая характеристика преступлений в сфере высоких технологий

1. **Задание 1 (Уровень: Понимание) – 20 минут.**
    - **"Концептуальный словарь своими словами"**. Опираясь на предоставленный теоретический материал и ваши лекционные записи, сформулируйте своими словами развернутые определения следующих понятий:
        - Информационные преступления (с указанием их групп).
        - Информационная преступность (укажите ее особенности и парадоксальные "положительные стороны").
        - Компьютерная информация (сравните легальное определение в РФ с международными подходами и предложенным "более правильным определением", укажите его ключевые свойства).
        - Основные угрозы в сфере высоких технологий (выберите 3 наиболее актуальные, на ваш взгляд, и кратко обоснуйте свой выбор).
        - Модель "as a service" в контексте киберпреступности.
    - *Обсуждение в малых группах (по 3-4 человека) и затем общее обсуждение.*
2. **Задание 2 (Уровень: Применение) – 30 минут.**
    - **"Классификатор угроз и деяний"**. Проанализируйте следующие гипотетические ситуации. Определите, к какой из "основных угроз в сфере высоких технологий" (согласно теоретическому

материалу) можно отнести каждую ситуацию и к какой группе информационных преступлений (специфически информационные; общеуголовные с существенным облегчением; общеуголовные с несущественным влиянием ИТ) можно отнести описанное деяние. Аргументируйте свой ответ.

- Ситуация А: Группа лиц систематически рассылает электронные письма от имени известного банка с просьбой перейти по ссылке и ввести данные банковской карты для "обновления системы безопасности". Полученные данные используются для хищения средств.
- Ситуация Б: Активисты движения за свободу информации взломали серверы крупной корпорации, обвиняемой в загрязнении окружающей среды, и опубликовали внутреннюю переписку руководства, подтверждающую факты нарушений.
- Ситуация В: Следствие установило, что организаторы договорных матчей координировали свои действия и передавали информацию о результатах через зашифрованный мессенджер.

- *Работа индивидуальная, затем обсуждение в парах и вынесение на общее обсуждение.*

3. **Задание 3 (Уровень: Анализ) – 30 минут.**
   - **"Дефиниции в фокусе: информация и ее безопасность"**.
     - Проанализируйте легальное определение информации (ФЗ "Об информации...") и определение компьютерной информации (примечание к ст. 272 УК РФ в редакции ФЗ № 420-ФЗ). Выделите сильные и слабые стороны определения компьютерной информации, данного в УК РФ, опираясь на критику, представленную в теоретическом материале.
     - Соотнесите понятия "общественная безопасность", "общественный порядок" (как родовой объект) и "информационная безопасность" (как видовой объект) преступлений главы 28 УК РФ. Объясните, почему именно информационная безопасность является видовым объектом данной группы преступлений, раскрыв ее ключевые составляющие (конфиденциальность, целостность, доступность).
   - *Работа в малых группах, подготовка кратких тезисов для общего обсуждения.*

Аудиторное занятие 2: Компьютерные преступления

1. **Задание 4 (Уровень: Понимание/Анализ) – 30 минут.**
   - **"Анатомия состава преступления"**. Используя текст Уголовного кодекса РФ и предоставленный теоретический

материал, детально разберите по элементам и признакам состав преступления, предусмотренный **ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ)**. Особое внимание уделите:

- Определению понятия "вредоносная компьютерная программа" и спорным вопросам его толкования (программы двойного назначения, взломщики паролей и т.д.).
- Характеристике объективной стороны (формы деяний, момент окончания для каждой из них).
- Субъективной стороне и содержанию умысла.
- Квалифицирующим признакам.

- *Работа индивидуальная. Преподаватель выборочно вызывает студентов для представления результатов.*

2. **Задание 5 (Уровень: Применение/Анализ) – 40 минут.**
   - **"Квалификационный практикум"**. Ознакомьтесь с фабулами.
     - Фабула 1: Системный администратор компании "Рога и копыта" Иванов, уволенный за прогулы, перед уходом с работы скопировал на флеш-накопитель базу данных клиентов компании, содержащую их персональные данные и историю заказов, а затем разместил объявление о ее продаже на одном из теневых форумов.
     - Фабула 2: Студент Петров из любопытства скачал из Интернета программу, предназначенную для подбора паролей к Wi-Fi сетям. Используя ее, он получил доступ к незащищенной сети своего соседа Сидорова и в течение месяца пользовался его интернетом для скачивания фильмов, чем причинил Сидорову ущерб в размере 1500 рублей (стоимость интернет-тарифа).
     - Фабула 3: Группа хакеров "Анонимус-Возмездие" осуществила DDoS-атаку на сайт государственного органа, отвечающего за экологический надзор, в знак протеста против выдачи разрешения на строительство вредного производства. Работа сайта была парализована на двое суток, что привело к невозможности для граждан подать электронные обращения и получить информацию. Ущерб оценен в 2 000 000 рублей из-за необходимости привлечения сторонних специалистов для восстановления работы и потерь от простоя сервисов.
   - Для каждой фабулы:
     - Предложите предварительную уголовно-правовую квалификацию деяния(ий) со ссылкой на конкретные статьи (части, пункты) УК РФ.

        - Укажите, какие признаки соответствующего состава (составов) преступления присутствуют в описанной ситуации.
        - Сформулируйте, какие дополнительные фактические обстоятельства необходимо установить для окончательной и точной квалификации.
        - Укажите, имеется ли в данном случае конкуренция уголовно-правовых норм и как она должна разрешаться.
    - *Работа в малых группах. Каждая группа анализирует одну фабулу, затем представляет свое решение для общего обсуждения и корректировки.*
3. **Задание 6 (Уровень: Синтез – подготовка к проекту) – 10 минут.**
    - **"Банк проблемных идей"**. На основе изученного материала (включая "спорные вопросы" по статьям УК РФ, недостатки определений), а также анализа фабул из Задания 5, каждая малая группа должна сформулировать 1-2 наиболее актуальные, на их взгляд, проблемы правоприменения или несовершенства законодательства в сфере компьютерных преступлений. Эти идеи могут стать основой для ваших мини-проектов.
    - *Краткое представление идей от каждой группы.*

Аудиторное занятие 3: Текущий контроль в форме подготовки мини-проекта по теме "Понятие и общая характеристика преступлений в сфере высоких технологий. Компьютерные преступления"

Задание 7 (Уровень: Синтез, Оценка, Получение нового опыта) – 80 минут.

- **"Разработка концепции мини-проекта"**.
    - **Этап 1 (15 минут):** Выбор темы. Студенты (индивидуально или в парах, по согласованию с преподавателем) выбирают одну из предложенных тем мини-проекта (см. фонд оценочных средств) или, по согласованию с преподавателем, формулируют собственную тему, основанную на идеях из "Банка проблемных идей" (Задание 6) или иных актуальных аспектах изученной темы.
    - **Этап 2 (50 минут):** Разработка структуры и содержания. Студенты определяют цель, задачи, актуальность выбранной темы, составляют предварительный план (структуру) проекта, подбирают ключевые нормативные акты, судебную практику и научные источники. Начинают формулировать основные тезисы и аргументы.
    - **Этап 3 (15 минут):** Консультации с преподавателем, обсуждение промежуточных результатов, корректировка планов.

- **Важно:** На аудиторном занятии осуществляется основная концептуальная проработка мини-проекта. **Окончательное оформление мини-проектов (в виде эссе, аналитической записки или презентации объемом 5-7 страниц/слайдов) осуществляется студентами после занятия в рамках самостоятельной работы.** Выполненный проект направляется преподавателю на электронную почту в установленный срок. Контроль выполнения осуществляется дистанционно.

Методические рекомендации по выполнению заданий:

- **Общие принципы:**
  - Внимательно изучайте предоставленный теоретический материал – он содержит ключ к пониманию многих аспектов темы.
  - Активно используйте текст Уголовного кодекса РФ (Глава 28 и др.), Федеральный закон "Об информации, информационных технологиях и о защите информации", Постановления Пленума Верховного Суда РФ по соответствующим вопросам.
  - Не бойтесь высказывать собственное мнение, но всегда аргументируйте его ссылками на нормы права, доктринальные источники или логические построения.
  - Работайте в команде: обсуждайте, делитесь идеями, критически оценивайте предложения друг друга.
- **Для заданий на понимание (Задание 1):**
  - Избегайте простого копирования текста. Старайтесь переформулировать определения своими словами, демонстрируя глубину осмысления материала.
  - Приводите собственные примеры, иллюстрирующие теоретические положения.
- **Для заданий на применение (Задание 2, Задание 5):**
  - При анализе фабул четко выделяйте юридически значимые обстоятельства.
  - Соотносите их с признаками конкретных составов преступлений, указанных в УК РФ.
  - При квалификации указывайте не только статью, но и часть, пункт (если применимо).
  - Обосновывайте необходимость установления дополнительных фактов для точной квалификации.
- **Для заданий на анализ (Задание 3, Задание 4):**
  - Разлагайте сложные понятия или правовые конструкции на составные элементы.
  - Сравнивайте различные подходы, определения, выявляя их сильные и слабые стороны.
  - Используйте таблицы, схемы для наглядного представления результатов анализа, если это уместно.

- **Для мини-проекта (Задание 7):**
    - **Целеполагание:** Четко сформулируйте цель и задачи вашего исследования.
    - **Структура:** Продумайте логическую структуру проекта (введение, основная часть с разделением на параграфы/разделы, заключение, список источников).
    - **Источники:** Используйте разнообразные источники: нормативные акты, судебную практику (решения судов различных инстанций, обобщения практики), научные статьи, монографии, учебную литературу.
    - **Аргументация:** Все выводы и предложения должны быть тщательно аргументированы.
    - **Оригинальность:** Стремитесь к самостоятельности суждений. Если выявляете проблему, предложите свой вариант ее решения.
    - **Оформление:** Соблюдайте требования к оформлению научных работ (ссылки, список литературы).

Примеры выполнения заданий (схематично):

- **Пример выполнения Задания 1 (фрагмент):**
    - *Понятие "Информационная преступность":* Это не просто сумма отдельных преступлений в IT-сфере, а целое социальное явление. Оно характеризуется тем, что преступники используют информационные технологии как основной инструмент или среду для совершения преступлений. Особенность в том, что она часто трансгранична, анонимна и требует от преступников специальных знаний. Парадоксально, но борьба с ней стимулирует развитие средств защиты информации, а иногда "хактивизм" может вскрывать общественно значимые проблемы, хотя формально и является преступлением.
- **Пример выполнения Задания 5 (фрагмент по Фабуле 1):**
    - *Предварительная квалификация:* Действия Иванова можно предварительно квалифицировать по ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности) и, возможно, по ст. 137 УК РФ (нарушение неприкосновенности частной жизни) или ст. 183 УК РФ (незаконные получение и разглашение сведений, составляющих коммерческую тайну), если база данных содержит соответствующие сведения.
    - *Признаки состава ст. 272 УК РФ:* Объект – безопасность компьютерной информации. Объективная сторона – неправомерное копирование охраняемой законом компьютерной информации (базы данных клиентов), что является одним из последствий, указанных в диспозиции. Субъект – Иванов,

достигший 16 лет. Субъективная сторона – прямой умысел, корыстная заинтересованность (продажа базы).
    - *Дополнительные обстоятельства:* Необходимо установить, была ли информация охраняемой законом (например, режим коммерческой тайны, защита персональных данных), был ли у Иванова правомерный доступ именно к этой базе в полном объеме или он превысил свои полномочия, был ли причинен крупный ущерб (для ч. 2 ст. 272 по этому основанию), каков точный характер информации в базе (персональные данные, коммерческая тайна).
    - *Конкуренция норм:* Возможна идеальная совокупность ст. 272 УК РФ и ст. 137 (или 183) УК РФ, если будут установлены все признаки соответствующих составов.
- **Пример выполнения мини-проекта (схематично по теме "Эволюция понятия "компьютерная информация"...")**
    - **Тема:** "Компьютерная информация" как ключевой элемент составов преступлений главы 28 УК РФ: проблемы законодательного определения и доктринального толкования.
    - **Цель:** Проанализировать эволюцию и текущее состояние понятия "компьютерная информация" в уголовном праве РФ, выявить его влияние на квалификацию и предложить пути совершенствования.
    - **Задачи:**
        1. Исследовать генезис понятия "компьютерная информация" в российском законодательстве.
        2. Проанализировать действующее легальное определение (примечание к ст. 272 УК РФ), его сильные и слабые стороны.
        3. Изучить подходы к толкованию данного понятия в доктрине и судебной практике.
        4. Выявить проблемы квалификации, связанные с несовершенством дефиниции.
        5. Разработать предложения по оптимизации законодательного определения.
    - **Структура (примерная):**
        - Введение (актуальность, цель, задачи, объект, предмет, методология).
        - Глава 1. Теоретико-правовые основы понятия "компьютерная информация".
            - 1.1. Международно-правовые подходы к определению компьютерной информации.
            - 1.2. Становление и развитие понятия "компьютерная информация" в российском законодательстве.

- Глава 2. Анализ действующего законодательства и практики его применения.
  - 2.1. Критический анализ легального определения компьютерной информации в УК РФ.
  - 2.2. Проблемы толкования и применения понятия в судебной практике (на примерах конкретных дел).
- Глава 3. Направления совершенствования уголовно-правового определения "компьютерной информации".
  - 3.1. Обоснование необходимости изменения действующей дефиниции.
  - 3.2. Предложения по новой редакции понятия "компьютерная информация" для целей УК РФ.
- Заключение (основные выводы и предложения).
- Список использованных источников.

3. Проверка практических заданий, выполненных обучающимися:

- **Процедура проверки:**
  - Устные ответы и участие в обсуждениях на занятиях (Задания 1-6) оцениваются преподавателем непосредственно в ходе занятия.
  - Выборочная проверка записей в рабочих тетрадях (конспектов ответов).
  - Проверка мини-проектов (Задание 7) осуществляется преподавателем после их предоставления студентами в электронном виде. Предоставляется обратная связь.
- **Шкала оценивания (классическая 5-балльная):**
  - **"Отлично" (5 баллов):** Студент демонстрирует глубокое и всестороннее понимание материала, свободно оперирует понятиями, способен самостоятельно анализировать сложные ситуации и формулировать аргументированные выводы. Ответы полные, точные, логичные. Мини-проект отличается оригинальностью (в рамках учебного задания), полнотой исследования, грамотным использованием источников и четкостью предложений. Продемонстрировано освоение всех заявленных индикаторов компетенций на высоком уровне.
  - **"Хорошо" (4 балла):** Студент в целом освоил материал, правильно отвечает на поставленные вопросы, умеет применять знания на практике, но допускает незначительные неточности или испытывает некоторые затруднения при анализе особо сложных аспектов. Мини-проект выполнен добросовестно, основные задачи решены, но могут быть отдельные недостатки в аргументации или полноте охвата проблемы. Индикаторы компетенций в основном освоены.
  - **"Удовлетворительно" (3 балла):** Студент имеет общее представление о теме, но допускает существенные ошибки, не

всегда может аргументировать свою позицию, показывает поверхностное понимание некоторых вопросов. Мини-проект выполнен формально, содержит неточности, не в полной мере раскрывает тему, есть проблемы с использованием источников или аргументацией. Освоены только базовые индикаторы компетенций.

- **"Неудовлетворительно" (2 балла):** Студент не освоил значительную часть материала, не может ответить на ключевые вопросы, демонстрирует фундаментальное непонимание темы. Мини-проект не представлен или выполнен на крайне низком уровне, не соответствует требованиям. Индикаторы компетенций не освоены.

Задания для самостоятельной работы по данной теме (после аудиторных занятий):

1. Проработайте Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"". Выпишите ключевые разъяснения, относящиеся к ст. 272-274.2 УК РФ.
2. Найдите и проанализируйте 2-3 актуальных (за последние 1-2 года) судебных решения (приговора) по ст. 272, 273 или 274.1 УК РФ. Обратите внимание на то, как суд устанавливает признаки состава преступления, какие доказательства использует, какие проблемы квалификации возникают.
3. Подготовьте краткое эссе (1-2 страницы) на тему: "Спорные вопросы отнесения программного обеспечения к категории "вредоносных компьютерных программ" (ст. 273 УК РФ): анализ доктрины и правоприменительной практики".

Список вопросов для самоконтроля:

1. Дайте определение понятию "преступления в сфере высоких технологий". Каковы их основные группы?
2. Раскройте содержание понятия "компьютерная информация" согласно УК РФ. Какие проблемы связаны с данным определением?
3. Каковы основные свойства информации, имеющие значение для уголовно-правовой квалификации?
4. Что понимается под информационной безопасностью? Каковы ее основные компоненты?
5. Назовите родовой и видовой объекты преступлений, предусмотренных главой 28 УК РФ.

6. В чем заключается объективная сторона состава преступления, предусмотренного ст. 272 УК РФ? Какие последствия являются обязательными для данного состава?
7. Дайте определение "вредоносной компьютерной программе". Какие действия с такими программами являются уголовно наказуемыми согласно ст. 273 УК РФ?
8. В чем заключается специфика объективной стороны преступления, предусмотренного ст. 274 УК РФ? Кто является субъектом данного преступления?
9. Что такое "критическая информационная инфраструктура Российской Федерации"? Какие деяния в отношении нее криминализированы в ст. 274.1 УК РФ?
10. В чем особенность конструкции состава преступления, предусмотренного ст. 274.2 УК РФ? Что такое административная преюдиция в данном контексте?
11. Какие основные угрозы в сфере высоких технологий актуальны на сегодняшний день?
12. В чем сущность модели "as a service" применительно к киберпреступной деятельности?
13. Какие "положительные стороны" информационной преступности выделяются в теоретическом материале? Согласны ли вы с такой постановкой вопроса? Аргументируйте.
14. В чем отличие компьютерной информации, представленной в виде "данных", от "программ"? Имеет ли это различие значение для квалификации?
15. Какие спорные вопросы квалификации неправомерного доступа к компьютерной информации (ст. 272 УК РФ) вы можете назвать?

4. Текущий контроль успеваемости по теме № 2

Текущий контроль успеваемости проводится в форме выполнения мини-проекта.

Шкала и критерии оценивания приведены в оценочных средствах по дисциплине «Преступления в сфере высоких технологий» для данной ОПОП ВО, которые размещены на официальном сайте университета по ссылке https://swsu.ru/sveden/education/eduop/.

ТЕМА № 3
ХИЩЕНИЯ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

I. ДИСТАНЦИОННАЯ ЧАСТЬ

Задания, выполняемые до начала первого практического занятия по теме № 3

Внеаудиторная (домашняя) самостоятельная работа обучающихся по освоению основных положений темы № 3: предварительное (до начала первого практического занятия по теме) самостоятельное изучение теоретического учебного контента по новой теме дисциплины, разработанного преподавателем и представленного в цифровом формате на портале do.swsu.ru

1.1 Ознакомьтесь с **инструкцией** о порядке организации самостоятельной работы по изучению данной темы и следуйте ей.

1.2. Прочитайте **перечень основных теоретических вопросов**, которые необходимо самостоятельно освоить, и **текст с изложением указанных вопросов**.

1.3 Работая с текстом, вносите по мере чтения необходимые записи в **опорный конспект**, который поможет вам запомнить главное.

Опорный конспект по теме № 3 «Хищения с использованием новых информационных технологий»

1. ЗАПОМИНАЕМ ГЛАВНОЕ

1.1 Впишите пропущенные слова, чтобы раскрыть содержание ключевых понятий и положений:

а) Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) по своей сути является новой формой хищения, где завладение имуществом сопряжено с проникновением в _____ среду, в которой осуществляются различного рода информационные операции, юридические последствия которых состоят в приобретении участниками оборота имущества в виде _____, _____ денежных средств, иных _____ прав.

б) Ключевыми способами совершения преступления, предусмотренного ст. 159.6 УК РФ, являются: 1) _____ компьютерной информации; 2) _____ компьютерной информации; 3) _____ компьютерной информации; 4) _____ компьютерной информации; а также иное _____ в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

в) Признак «вмешательство в функционирование» по ст. 159.6 УК РФ следует рассматривать как критерий, существенно _____ пределы действия нормы. Простое получение доступа к информации (например, к паролям и логинам) без фактического воздействия на процессы _____, _____ и _____ информации, не образует данный признак.

г) Если лицо использует чужие учетные данные для хищения денежных средств (независимо от способа их получения), но при этом не осуществляет ввода, удаления, блокирования, модификации компьютерной информации или иного вмешательства в функционирование систем, содеянное следует квалифицировать по ст. _____ УК РФ.

д) КИБЕРВЫМОГАТЕЛЬСТВО – это требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой, как правило, связанной с _____ доступа к информации пользователя, ее _____, _____ или _____.

е) Основные механизмы кибервымогательства включают заражение информационной системы _____, которое может быть

как _____ (атака на конкретную жертву с учетом ее особенностей), так и осуществляться методами _____ заражения (например, через ботнеты или зараженные веб-сайты).

ж) Сложность квалификации посягательств на виртуальные «вещи» (например, игровые артефакты) обусловлена тем, что они традиционно не признаются _____ в смысле гражданского и уголовного права, а их экономический оборот зачастую _____ правилами операторов соответствующих систем.

з) КРИПТОВАЛЮТА – это разновидность _____ валюты, учёт внутренних расчётных единиц которой обеспечивает _____ платёжная система, работающая в полностью _____ режиме, а ее безопасность основана на _____ методах.

1.2 Установите соответствие между уголовно-правовой нормой (или предлагаемым решением) и описанием ситуации. Соедините их стрелками или укажите соответствующую букву рядом с цифрой:

А) Ст. 159.6 УК РФ (Мошенничество в сфере компьютерной информации) Б) Ст. 158 УК РФ (Кража, при определенных условиях) В) Ст. 272 УК РФ (Неправомерный доступ к компьютерной информации) Г) Предлагаемая специальная норма об ответственности за кибервымогательство Д) Ст. 179 УК РФ (Принуждение к совершению сделки или к отказу от ее совершения)

1. _____ Получение доступа к аккаунту в онлайн-игре и изменение информации о принадлежности виртуальных предметов, без их последующей продажи за реальные деньги, но с блокированием доступа законному пользователю.
2. _____ Требование уплаты денежных средств под угрозой распространения компрометирующих сведений, полученных путем взлома электронной почты. (Примечание: рассмотрите в контексте специфики киберугроз)
3. _____ Хищение денежных средств путем внедрения в банковскую систему вредоносного ПО, которое изменяет реквизиты получателя в платежных поручениях.
4. _____ Использование логина и пароля, добровольно сообщенных знакомым, для входа в его онлайн-банк и перевода денег на свой счет, без изменения работы самой системы.
5. _____ Принуждение под угрозой физической расправы к передаче дорогостоящих скинов в компьютерной игре, которые были приобретены за реальные деньги и могут быть обменены на другие игровые ценности.

1.3 Укажите стрелочкой ОДНО наиболее точное утверждение, отражающее позицию законодателя и судебной практики относительно состава преступления, предусмотренного ст. 159.6 УК РФ:

Объективная сторона ст. 159.6 УК РФ охватывает:

Любое незаконное получение сведений, содержащихся на компьютерных носителях, если это привело к материальному ущербу.

Только такие действия, которые вызывают физическое повреждение компьютерного оборудования или сетей.

Вмешательство именно в *функционирование* средств хранения, обработки или передачи компьютерной информации (или сетей), повлекшее хищение.

Распространение в компьютерных сетях заведомо ложных сведений с целью хищения имущества (что скорее относится к ст. _____ УК РФ).

1.4 Перечислите виды кибервымогательства, рассмотренные в лекции, и их ключевые отличительные черты:

1. Вид:
   _____
   Ключевые черты:
   _____

2. Вид:
   _____
   Ключевые черты:
   _____

2. АНАЛИЗ ПРАКТИКИ И ПРОБЛЕМЫ КВАЛИФИКАЦИИ

2.1 Заполните таблицу, кратко описав фабулу дела (или типичную ситуацию) и основную проблему уголовно-правовой квалификации, обсуждавшуюся в лекции:

№	Краткое описание казуса/ситуации	Основная проблема квалификации
1	Лицо получает доступ к файлу с паролями на чужом компьютере, но задерживается до того, как успевает использовать их для хищения средств и вмешаться в работу банковской системы.	Будет ли в данном случае оконченный состав или покушение на ст. 159.6 УК РФ? Почему? _____
2	«Хищение» виртуальных танков в игре World of Tanks путем неправомерного доступа к аккаунту и их последующая перепродажа за реальные деньги. (Дело Дмитрия Ш.)	По какой статье УК РФ было осуждено лицо? Является ли такая квалификация исчерпывающей с точки зрения общественной опасности и природы «похищенного»? _____
3	Угроза пистолетом и требование передать виртуальные ножи (Counter Strike), купленные за значительную сумму. (Случай в Красноярске)	Почему квалификация по ст. 162 УК РФ («Разбой») была признана несостоятельной? Какая альтернативная квалификация была предложена и на чем она основана? _____
4	Вымогательство криптовалюты под угрозой уголовного преследования, инсценировка задержания. (Дело Пирона и Пригожина)	Какова была первоначальная позиция суда первой инстанции относительно криптовалюты как предмета преступления? Какое решение в итоге принял кассационный суд и подтвердил суд первой инстанции при новом рассмотрении? _____

2.2 Заполните пропуски, отражая предлагаемые в лекции подходы к решению сложных вопросов квалификации:

а) Для эффективного противодействия кибервымогательству предлагается введение в УК РФ _____ нормы, устанавливающей ответственность за требование передачи чужого имущества или права на имущество под угрозой _____, _____ или _____ компьютерной информации, либо нарушения функционирования информационных систем.

б) Квалифицирующими признаками для предлагаемой нормы о кибервымогательстве могли бы стать: 1) Наступление _____ последствий (в т.ч. крупный материальный ущерб); 2) Нарушение функционирования информационных систем, имеющих _____ значение; 3) _____ характер преступных действий.

в) При квалификации посягательств на виртуальные предметы, когда отсутствует прямое вмешательство в информационную систему, а воздействие оказывается на пользователя, можно рассматривать передачу такого предмета как

_____ права требования к разработчику/оператору игры. В этом случае деяние, совершенное под принуждением, может быть квалифицировано по ст. _____ УК РФ.

2.3 Соотнесите понятия и их определения/характеристики. Впишите соответствующую букву рядом с цифрой:

1. _____ Вмешательство в функционирование ИС
2. _____ Модификация компьютерной информации
3. _____ Блокирование компьютерной информации
4. _____ Криптовалюта как предмет преступления

А. Внесение изменений в существующую компьютерную информацию. Б. Совокупность технических и программных средств, предназначенных для автоматизации процессов сбора, обработки, хранения и передачи информации. (Примечание: это общее определение, но в контексте – то, на что воздействуют). В. Признак объективной стороны ст. 159.6 УК РФ, означающий целенаправленное воздействие на процессы обработки, хранения и передачи информации, нарушающее их штатный режим. Г. Невозможность или затруднение доступа к компьютерной информации либо ее использования. Д. Объект гражданских прав, который может быть предметом хищения, что подтверждено судебной практикой по конкретным делам.

3. РЕФЛЕКСИЯ

3.1 Сформулируйте кратко основной вывод, который Вы сделали лично для себя после изучения темы «Хищения с использованием новых информационных технологий»: ВЫВОД ЛИЧНО ДЛЯ СЕБЯ:

1.4 Посмотрите **видеоролик** по теме № 3 в ходе чтения текста (параллельно с ним).

Обратите внимание на необходимость разграничения составов преступлений, связанных с неправомерным доступом к компьютерной информации и хищением виртуального имущества, от принуждения к совершению сделки в контексте посягательств на виртуальные объекты, а также на дискуссионный вопрос признания криптовалюты предметом хищения в уголовно-правовом смысле.

1.5 Перескажите изученный теоретический материал по вопросам, указанным в инструкции, и опорному конспекту. Воспользуйтесь также следующими **вопросами для самоконтроля**:

1. В чем заключается принципиальное отличие мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) от традиционного понимания мошенничества?
2. Какие способы совершения мошенничества в сфере компьютерной информации перечислены в статье 159.6 УК РФ?
3. Что понимается под "вмешательством в функционирование" средств хранения, обработки или передачи компьютерной информации, и почему этот признак важен для квалификации преступления по ст. 159.6 УК РФ?

4. В каких случаях требуется дополнительная квалификация действий виновного по статьям 272, 273, 274.1 УК РФ при совершении мошенничества в сфере компьютерной информации?
5. Что такое кибервымогательство, и какие основные виды кибервымогательства существуют?
6. Почему кибервымогательство представляет собой комплексное преступление, и какие составы преступлений оно может включать?
7. Каковы основные проблемы квалификации хищений виртуального имущества в онлайн-играх?
8. Почему квалификация хищения виртуальных предметов как разбоя (ст. 162 УК РФ) признается несостоятельной?
9. Каким образом можно квалифицировать действия лица, похитившего виртуальные предметы, с точки зрения принуждения к совершению сделки (ст. 179 УК РФ)?
10. В чем особенность криптовалюты как объекта преступных посягательств?
11. Каковы особенности доказывания и квалификации хищения криптовалюты, учитывая ее правовой статус в РФ?
12. Какие квалифицирующие признаки кибервымогательства, требующие применения суровых мер уголовной ответственности, вы можете назвать?

1.6 Возьмите с собой на практическое занятие свой **опорный конспект** по теме № 3.

1.7 Выполните **входное тестирование** по теме № 3.

Ответьте на вопросы и выполните задания в тестовой форме по теме № 3:

I. Вопросы в закрытой форме (выберите один правильный вариант ответа):

1. В чем заключается принципиальное отличие преступления, предусмотренного ст. 159.6 УК РФ, от традиционного мошенничества (ст. 159 УК РФ) с точки зрения объекта воздействия при хищении? а) Обман или злоупотребление доверием направлены исключительно на автоматизированные системы. б) Завладение имуществом сопряжено с проникновением в информационную среду, где осуществляются информационные операции. в) Предметом преступления всегда выступают исключительно безналичные денежные средства. г) Обязательным признаком является использование вредоносного программного обеспечения. д) Преступление совершается только в отношении юридических лиц.
2. Какой из перечисленных способов совершения преступления, предусмотренного ст. 159.6 УК РФ, НЕ указан в диспозиции статьи как непосредственное действие с компьютерной информацией? а) Ввод

компьютерной информации. б) Удаление компьютерной информации. в) Копирование компьютерной информации. г) Блокирование компьютерной информации. д) Модификация компьютерной информации.

3. Что, согласно представленному материалу, НЕ будет образовывать признаков объективной стороны компьютерного мошенничества (ст. 159.6 УК РФ), если умысел на хищение не был доведен до конца? а) Целенаправленное программное воздействие на серверы, нарушившее процесс обработки информации. б) Получение доступа к логинам и паролям для управления счетом через систему «банк-клиент» путем простого ознакомления с файлом на компьютере пользователя без фактического вмешательства в функционирование системы. в) Модификация компьютерной информации, приведшая к незаконному перечислению средств. г) Блокирование компьютерной информации, сделавшее невозможным доступ законного пользователя к своим средствам. д) Ввод ложной информации в систему, повлекший неправомерное приобретение права на имущество.
4. Какой вид кибервымогательства, согласно тексту, является более опасным и часто ставит жертву в безвыходное положение? а) Блокирование доступа к системе с демонстрацией порнографических изображений. б) Требование уплаты «штрафа» от имени правоохранительных органов за якобы совершенные нелегальные действия. в) Использование криптографических средств для шифрования информации пользователя с требованием выкупа за ключ расшифровки. г) Угроза распространения компрометирующих сведений, полученных из информационной системы. д) Массовое заражение компьютеров с использованием ботнетов с целью показа навязчивой рекламы.
5. Какую статью УК РФ, по мнению автора материала, целесообразно было бы применить для квалификации случая в Красноярске (2016 г.), где у участника турнира по Counter Strike под угрозой пистолета требовали передать виртуальные предметы, учитывая специфику «виртуального имущества» как права требования? а) Ст. 162 УК РФ «Разбой». б) Ст. 163 УК РФ «Вымогательство». в) Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». г) Ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». д) Ст. 179 УК РФ «Принуждение к совершению сделки или отказу от её совершения».
6. Какое решение принял третий кассационный суд в деле Пирона и Пригожина относительно правового статуса криптовалюты? а) Подтвердил, что криптовалюта не является объектом гражданских прав и предметом преступления. б) Признал криптовалюту платежным средством и вернул дело на новое рассмотрение. в) Указал на необходимость квалификации деяния только в части хищения наличных

денег. г) Отменил приговор и прекратил уголовное дело в части криптовалюты. д) Признал криптовалюту информацией, не имеющей стоимостного выражения.

7. Использование чужих учетных данных для доступа к онлайн-банку и последующего хищения средств, если сам доступ был получен без вмешательства в функционирование компьютерной системы (например, пароль был подсмотрен или добровольно сообщен), согласно тексту, следует квалифицировать как: а) Ст. 159.6 УК РФ. б) Ст. 158 УК РФ. в) Ст. 272 УК РФ. г) Ст. 159 УК РФ. д) Ст. 165 УК РФ.

II. Вопросы в открытой форме (впишите пропущенное слово или словосочетание):

8. Согласно представленному материалу, преступление, предусмотренное статьей 159.6 УК РФ, по сути, является новой формой хищения, когда завладение имуществом сопряжено с проникновением в _____, в которой осуществляются различного рода информационные операции.
9. Ключевым признаком объективной стороны преступления, предусмотренного ст. 159.6 УК РФ, ограничивающим пределы действия нормы, является «_____ в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей».
10. Кибервымогательство, согласно определению, – это разновидность информационного преступления, сущность которого заключается в том, что преступник вымогает у потерпевшего денежные средства или иные предметы, имеющие материальную ценность, используя угрозы, как правило, связанные с _____ к информации пользователя.
11. В подавляющем большинстве дел о «хищении» виртуального имущества фактически речь идёт о неправомерном (с использованием чужих учётных данных) доступе к компьютерной информации, который влечёт последствия в виде блокирования доступа к ней законного пользователя и _____ записей в базе данных компьютерной игры.
12. Криптовалюта – это разновидность цифровой валюты, учёт внутренних расчётных единиц которой обеспечивает _____ платёжная система, работающая в полностью автоматическом режиме.
13. Предлагается включение в уголовное законодательство специальной нормы, устанавливающей ответственность за кибервымогательство, то есть требование передачи чужого имущества под угрозой уничтожения, повреждения или блокирования компьютерной информации, нарушения функционирования _____.

III. Вопросы на установление правильной последовательности:

14. Расположите в правильной последовательности этапы аргументации суда по делу Пирона и Пригожина относительно криптовалюты, согласно тексту:
    1. Третий кассационный суд заявил, что криптовалюта является платежным средством.
    2. Итоговый приговор Петроградского суда включил 55 млн рублей в криптовалюте.
    3. Петроградский суд счел, что криптовалюта не является средством платежа и предметом преступления.
    4. Дело возвращено на новое рассмотрение в суд первой инстанции.
15. Расположите в хронологической последовательности этапы развития проблемы посягательств на виртуальное имущество, как это описано в тексте:
    1. Массовое появление онлайн-игр с моделью free to play и платным контентом.
    2. Первые зафиксированные случаи «виртуальных» хищений в онлайн-играх (конец 1990-х – начало 2000-х).
    3. Попадание противоправных деяний, связанных с играми типа World of Tanks, в поле зрения правоохранительных органов.
    4. Появление возможности приобретать игровое имущество за реальные деньги в играх типа Ultima Online.
16. Расположите в логической последовательности шаги, которые, согласно примеру из текста, могут быть расценены как вмешательство в функционирование информационной среды при совершении преступления по ст. 159.6 УК РФ:
    1. Завладение денежными средствами путем перечисления на подконтрольные счета через электронную систему "*-Онлайн".
    2. Получение информации о счетах граждан.
    3. Использование полученных сим-карт и паролей.
    4. Изготовление поддельных доверенностей и получение дубликатов сим-карт и паролей.
17. Расположите в логической последовательности действия при совершении кибервымогательства с использованием шифрования данных:
    1. Требование уплаты вознаграждения за предоставление ключа для расшифровки.
    2. Заражение информационной системы вредоносным программным обеспечением.
    3. Шифрование информации пользователя.
    4. Получение (или неполучение) ключа для расшифровки данных после уплаты (или неуплаты) выкупа.

IV. Вопросы на установление соответствия:

18. Установите соответствие между статьями Уголовного кодекса РФ и их кратким описанием применительно к контексту хищений с использованием информационных технологий: А) Ст. 159 УК РФ Б) Ст. 159.6 УК РФ В) Ст. 272 УК РФ Г) Ст. 158 УК РФ (в контексте использования чужих учетных данных)
    1. Хищение путем ввода, удаления, блокирования, модификации компьютерной информации или иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации.
    2. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.
    3. Хищение, совершаемое путем обмана или злоупотребления доверием физического лица (например, при распространении в компьютерных сетях заведомо ложных сведений).
    4. Тайное хищение чужого имущества с использованием полученных (без вмешательства в функционирование систем) чужих учетных данных.
19. Установите соответствие между видом кибервымогательства и его характерной чертой: А) Блокирование доступа к системе без вмешательства в данные Б) Кибервымогательство с использованием криптографических средств
    1. Рассчитано на неподготовленных пользователей, использует приемы психологического давления (например, демонстрация порнографии или сообщения от имени «правоохранительных органов»).
    2. Зачастую ставит жертву в безвыходное положение, так как восстановление информации без ключа шифрования невозможно.
    3. Преступники не всегда предоставляют ключ для расшифровки даже после уплаты выкупа.
    4. Потенциальный ущерб связан в большей степени со стрессом и смущением пользователя, чем с безвозвратной потерей данных.
20. Установите соответствие между проблемой квалификации деяния и возможным/предлагаемым подходом к ее решению, описанным в тексте: А) Хищение виртуальных игровых предметов путем физического принуждения игрока Б) Хищение криптовалюты путем вымогательства В) Кибервымогательство (в целом)
    1. Предложение о введении специальной нормы в УК РФ, устанавливающей ответственность за требование передачи имущества под угрозой воздействия на компьютерную информацию.

2. Признание криптовалюты платежным средством и предметом преступления (на основе судебной практики).
3. Возможная квалификация по ст. 179 УК РФ «Принуждение к совершению сделки или отказу от её совершения», рассматривая виртуальный предмет как право требования.
4. Квалификация по совокупности статей о компьютерных преступлениях и преступлениях против собственности.

21. Установите соответствие между способом совершения преступления, предусмотренного ст. 159.6 УК РФ, и его содержанием: А) Ввод компьютерной информации Б) Модификация компьютерной информации В) Блокирование компьютерной информации
    1. Изменение существующей в системе информации на ложную или искаженную.
    2. Сделание информации недоступной для законного пользователя.
    3. Добавление в систему не существовавшей ранее информации, не соответствующей действительности.
    4. Полное стирание информации из системы.
22. Установите соответствие между квалифицирующим признаком, предлагаемым для специальной нормы о кибервымогательстве, и его сутью: А) Наступление тяжких последствий Б) Массовый характер преступных действий В) Причинение крупного материального ущерба
    1. Охват преступной деятельностью большого числа потерпевших.
    2. Нарушение функционирования информационных систем, имеющих стратегическое значение.
    3. Стоимостное выражение похищенного или поврежденного имущества, превышающее установленный законом порог.
    4. Совершение преступления организованной группой.
23. Установите соответствие между термином, используемым в контексте киберпреступлений, и его определением/описанием: А) Вредоносное программное обеспечение (ВПО) Б) Ботнет В) Криптовалюта
    1. Сеть компьютеров, зараженных специальной программой, позволяющей злоумышленнику удаленно управлять ими без ведома владельцев.
    2. Разновидность цифровой валюты, учёт которой обеспечивает децентрализованная платёжная система.
    3. Программное обеспечение, предназначенное для несанкционированного доступа, уничтожения, блокирования, модификации, копирования информации или нарушения работы компьютерных систем.
    4. Система криптографической защиты данных.
24. Установите соответствие между описанной ситуацией и наиболее вероятной или обсуждаемой в тексте уголовно-правовой квалификацией: А) Лицо получило доступ к файлу с паролями на чужом

компьютере, но было задержано до использования этих паролей для хищения. Б) Распространение в компьютерных сетях заведомо ложных сведений с целью хищения денег у доверчивых граждан. В) Использование чужих учетных данных, полученных путем их подсматривания, для перевода денег со счета потерпевшего.

1. Отсутствие признаков объективной стороны ст. 159.6 УК РФ (покушения на компьютерное мошенничество).
2. Ст. 158 УК РФ.
3. Ст. 159 УК РФ.
4. Ст. 273 УК РФ.

25. Установите соответствие между элементом механизма защиты криптовалюты и его функцией: А) Цифровая подпись на основе системы с открытым ключом Б) Последовательное хеширование пакетов транзакций
    1. Обеспечивает невозможность изменения информации о количестве криптовалюты в уже сформированных блоках.
    2. Подтверждает полномочия на операции с адресом, гарантируя, что распоряжение доступно исключительно обладателю секретного ключа.
    3. Шифрует информацию о сумме транзакции.
    4. Генерирует новый адрес для каждой транзакции.

II. АУДИТОРНАЯ ЧАСТЬ

Практическое занятие № 3
«Хищения с использованием новых информационных технологий»

Цель практического занятия – приобретение обучающимися практического опыта в применении знаний, полученных при самостоятельном освоении темы № 3, в производственных ситуациях.

Планируемые результаты обучения:

Знать:	**Уметь:**	**Иметь опыт деятельности:**
содержание норм, устанавливающих ответственность за преступные деяния, связанные с преступлениями в сфере высоких технологий,	использовать информацию о нормах, устанавливающих ответственность за преступления в сфере высоких технологий, в целях их реализации; применять нормы особенной части	по обобщению и анализу информации, имеющей значение для реализации правовых норм в сфере установления ответственности за преступления в сфере высоких технологий;

особенности их реализации; методологические основы реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; содержание постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, связанных с уголовно-правовым регулированием ответственности за преступления в сфере высоких технологий; особенности оценки на соответствие признакам преступления (квалификации) конкретных преступлений в сфере высоких технологий, предусмотренных уголовным законодательством; способы толкования норм уголовного законодательства, позволяющие вычленить из их текста основные юридически

уголовного права, регулирующие ответственность за преступления в сфере высоких технологий; применять нормы особенной части уголовного права, регулирующие ответственность за преступления в сфере высоких технологий с учётом постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований; давать полную и точную квалификацию преступлений в сфере высоких технологий, с учётом положений Общей и Особенной части уголовного законодательства, разъяснений Пленума Верховного Суда РФ; толковать положения актов уголовного законодательства, касающиеся высоких технологий, основываясь на общих принципах толкования нормативных актов; разъяснять содержание норм уголовного законодательства, предусматривающих

по реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по обобщению и анализу постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, касающихся норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по принятию решений, связанных с оценкой на соответствие конкретных деяний, связанных с высокими технологиями, признакам преступления; по применению основных подходов к толкованию норм уголовного законодательства Российской Федерации, касающихся высоких технологий, и

значимые признаки преступных деяний, связанных с высокими технологиями, и сопоставить их с признаками преступления; особенности толкования норм уголовного законодательства, устанавливающих ответственность за конкретные преступления в сфере высоких технологий, позволяющие разграничить между собой смежные составы преступлений при наличии конкуренции норм	ответственность за совершение конкретных преступлений в сфере высоких технологий, с учётом судебной практики и доктрины уголовного права; устанавливать содержание оценочных признаков норм уголовного законодательства, регулирующих ответственность за преступления в сфере высоких технологий, а также признаков, позволяющих разграничить между собой смежные преступные деяния при наличии конкуренции норм	вычленению признаков конкретного деяния; по выявлению точного содержания норм уголовного законодательства, устанавливающих общие условия уголовной ответственности и освобождения от неё, а также признаки конкретных составов преступлений, связанных с преступлениями в сфере высоких технологий; по применению приёмов научного мышления, позволяющих устанавливать смысл нормоустановлений уголовно-правового характера, касающихся высоких технологий, в условиях правовой неопределённости, коллизий правового регулирования, конкуренции норм

Необходимое материально–техническое оборудование: ноутбук и (или) мобильные устройства преподавателя и обучающихся.

ПЛАН ПРАКТИЧЕСКОГО ЗАНЯТИЯ № 3

1. Уточнение и (или) углубление отдельных вопросов по теме № 3.
2. Выполнение обучающимися практических заданий.
3. Проверка практических заданий, выполненных обучающимися.
4. Текущий контроль успеваемости по теме № 3

1. Уточнение и (или) углубление отдельных вопросов по теме № 3
Консультация преподавателя

Студенты методом мозгового штурма формируют перечень вопросов, которые при самостоятельном освоении темы дома или при тестировании остались для них непонятными или показались сложными и (или) спорными. Преподаватель по результатам тестирования при необходимости добавляет в сформированный обучающимися список вопросы, которые, с его точки зрения, требуется уточнить или углубить.

Определяя с помощью поднятых рук количество студентов, считающих сложным конкретный вопрос из сформированного списка, преподаватель устанавливает вопросы, по которым сразу же проводит групповую консультацию.

Если в пояснениях нуждаются 1-2 человека, преподаватель индивидуально консультирует их в ходе практического занятия.

2. Выполнение обучающимися практических заданий

На данном практическом занятии выполнение обучающимися практических заданий проводится **по технологии ротации станций.**

Аудиторное занятие 1: Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ)

Аудитория разделена на 3 станции. Учебная группа делится на 3 малых группы, в каждой группе – 3-5 человек. На станции № 1 группа работает с преподавателем (ответы обучающихся на вопросы преподавателя по изучаемой теме и групповая и (или) индивидуальная консультация). На станции № 2 группа самостоятельно выполняет одно общее практическое задание. На станции № 3 все члены группы выполняют индивидуальные, но однотипные задания. Задания на станциях разные. На данном практическом занятии все задания направлены на **понимание** основных положений темы; **применение** знаний, умений и навыков в производственной ситуации; **анализ** информации или каких-либо данных. Время работы группы на одной станции – **25 минут**. По истечении указанного времени группы переходят по часовой стрелке на следующую станцию для выполнения другого практического задания. В течение практического занятия каждая группа проходит все станции и выполняет все практические задания.

Вопросы для работы на станции № 1 с преподавателем (по содержанию темы, изученному дома самостоятельно с использованием предоставленного теоретического материала):

1. Раскройте понятие "компьютерная информация" применительно к ст. 159.6 УК РФ. Какие виды информации могут быть предметом данного преступления?
2. Объясните своими словами, что понимается под "вводом, удалением, блокированием, модификацией компьютерной информации" как

способом совершения мошенничества в сфере компьютерной информации. Приведите примеры каждого из этих действий.

3. В чем заключается принципиальное отличие состава, предусмотренного ст. 159.6 УК РФ, от традиционного мошенничества (ст. 159 УК РФ)? Почему законодатель выделил его в отдельную норму?
4. Проанализируйте термин "вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей". Является ли простое использование чужих учетных данных для доступа к онлайн-банкингу таким вмешательством? Обоснуйте свой ответ, опираясь на предоставленный теоретический материал и Постановления Пленума ВС РФ (если имеются по данной теме).
5. Каковы критерии разграничения ст. 159.6 УК РФ и ст. 158 УК РФ (кража с банковского счета), если хищение денежных средств происходит с использованием банковских карт или систем дистанционного банковского обслуживания?
6. Требуется ли дополнительная квалификация действий виновного по ст. 272, 273, 274.1 УК РФ при совершении преступления, предусмотренного ст. 159.6 УК РФ? В каких случаях?

Практическое задание для станции № 2 (общее).

Фабула: Гражданин Сидоров, работая системным администратором в компании "ТехноСтрой", обнаружил уязвимость в системе бухгалтерского учета, позволяющую изменять реквизиты получателей платежей в формируемых платежных поручениях без ведома главного бухгалтера. Воспользовавшись этим, Сидоров в течение месяца периодически изменял реквизиты в нескольких платежных поручениях, направляемых контрагентам, на реквизиты своего личного счета и счета своего знакомого Петрова (который не был осведомлен о преступных намерениях Сидорова). В результате на счета Сидорова и Петрова было перечислено в общей сложности 750 000 рублей, принадлежащих ООО "ТехноСтрой". После каждого успешного перевода Сидоров восстанавливал исходные данные в системе, чтобы скрыть следы своих действий, однако не удалял логи доступа.

Задание:

1. Проанализируйте действия Сидорова.
2. Определите, имеются ли в его действиях признаки состава преступления, предусмотренного ст. 159.6 УК РФ. Обоснуйте свой ответ, указав на конкретные признаки объективной и субъективной стороны.
3. Рассмотрите, возможно ли квалифицировать действия Сидорова по иным статьям УК РФ (например, ст. 158, 159, 160 УК РФ). Аргументируйте, почему ст. 159.6 УК РФ является предпочтительной (или нет) в данном случае.

4. Определите, какие из действий Сидорова могут быть охарактеризованы как "ввод", "удаление", "блокирование" или "модификация" компьютерной информации, а также "вмешательство в функционирование".

Практические задания для станции № 3 (индивидуальные). Каждому студенту предлагается одна из следующих ситуаций. Необходимо:

- Кратко описать объективную сторону предполагаемого преступления.
- Указать, какие именно действия подпадают под "ввод, удаление, блокирование, модификацию компьютерной информации" или "иное вмешательство".
- Предложить предварительную квалификацию содеянного со ссылкой на часть и статью УК РФ.

1. **Задание для студента 1:** Хакер получил несанкционированный доступ к базе данных интернет-магазина и изменил цены на дорогостоящие товары на минимальные, после чего оформил заказ на свое имя и оплатил его по заниженной цене. Товары были ему доставлены.
2. **Задание для студента 2:** Сотрудница банка, имея легальный доступ к банковской системе, перевела денежные средства со счета клиента на свой счет, создав фиктивное расходное поручение в электронной системе.
3. **Задание для студента 3:** Злоумышленник разослал электронные письма от имени известного банка с ссылкой на поддельный сайт, где пользователи вводили свои логины и пароли от онлайн-банкинга. Получив эти данные, он вошел в личные кабинеты нескольких клиентов и перевел их средства на свои счета.
4. **Задание для студента 4:** Программист внедрил в систему онлайн-казино вредоносный код, который обеспечивал ему выигрыш в определенных играх. Полученные таким образом виртуальные средства он конвертировал в реальные деньги через платежную систему.
5. **Задание для студента 5:** Лицо, зная логин и пароль своего знакомого от мобильного приложения банка (знакомый сам ранее сообщил ему эти данные для совершения совместной покупки), без разрешения последнего вошел в приложение и перевел денежные средства на свой счет.

Аудиторное занятие 2: Кибервымогательство

Аудитория разделена на 3 станции. Учебная группа делится на 3 малых группы, в каждой группе – 3-5 человек. На станции № 1 группа работает с преподавателем (ответы обучающихся на вопросы преподавателя по изучаемой теме и групповая и (или) индивидуальная консультация). На станции № 2 группа самостоятельно выполняет одно общее практическое задание. На станции № 3 все члены группы выполняют индивидуальные, но однотипные задания. Задания на станциях разные. На данном практическом занятии все задания направлены на **понимание** основных положений темы;

анализ информации; **синтез** информации и **проведение оценки**. Время работы группы на одной станции – **25 минут**. По истечении указанного времени группы переходят по часовой стрелке на следующую станцию для выполнения другого практического задания. В течение практического занятия каждая группа проходит все станции и выполняет все практические задания.

Вопросы для работы на станции № 1 с преподавателем (по содержанию темы, изученному дома самостоятельно с использованием предоставленного теоретического материала):

1. Дайте определение кибервымогательства, опираясь на предоставленный теоретический материал. В чем его сущность и отличие от "классического" вымогательства (ст. 163 УК РФ)?
2. Какие основные механизмы и технологии используются кибервымогателями для достижения своих преступных целей? Приведите примеры.
3. Охарактеризуйте основные виды кибервымогательства, упомянутые в теоретическом материале (блокирование доступа без шифрования, шифрование данных). Какой из них, по вашему мнению, представляет большую общественную опасность и почему?
4. Почему кибервымогательство рассматривается как комплексное преступление? Какие составы преступлений УК РФ оно может в себя включать?
5. Обсудите проблемы квалификации кибервымогательства по действующему российскому уголовному законодательству. Достаточно ли существующих норм для эффективного противодействия этому явлению?
6. Какие аргументы можно привести в пользу введения специальной нормы об ответственности за кибервымогательство в УК РФ? Какие квалифицирующие признаки могли бы быть предусмотрены для такой нормы?

Практическое задание для станции № 2 (общее).

Ситуация: В крупную логистическую компанию "ТрансКарго" поступило электронное письмо с требованием уплатить 10 биткоинов. В противном случае авторы письма угрожали опубликовать в открытом доступе коммерческую тайну компании (базы данных клиентов, условия договоров с партнерами, финансовую отчетность), доступ к которой они, по их утверждению, получили в результате взлома серверов компании. В качестве доказательства к письму был приложен скриншот фрагмента внутренней переписки топ-менеджеров. Руководство "ТрансКарго" обратилось в правоохранительные органы. В ходе предварительной проверки было установлено, что серверы компании действительно подверглись атаке, и часть информации была скопирована.

Задание:

1. Проанализируйте данную ситуацию с точки зрения уголовного права.

2. Оцените, можно ли квалифицировать действия злоумышленников по ст. 163 УК РФ (Вымогательство). Аргументируйте свой ответ, обращая внимание на предмет вымогательства и характер угрозы.
3. Рассмотрите возможность квалификации содеянного по другим статьям УК РФ (например, ст. 272, 183, 137 УК РФ). Будет ли такая квалификация исчерпывающей?
4. Если бы злоумышленники требовали деньги под угрозой шифрования всех данных на серверах компании и блокирования ее работы, изменилась бы ваша оценка и возможная квалификация? Почему?
5. Предложите оптимальный, на ваш взгляд, вариант уголовно-правовой оценки действий злоумышленников в первоначальной ситуации, исходя из действующего УК РФ, и укажите его недостатки.

Практические задания для станции № 3 (индивидуальные). Каждому студенту предлагается разработать предложения по совершенствованию уголовного законодательства в части противодействия кибервымогательству. Необходимо:

- Сформулировать диспозицию предлагаемой новой статьи (или части статьи) УК РФ, предусматривающей ответственность за кибервымогательство.
- Предложить не менее двух квалифицирующих признаков для данной нормы.
- Кратко обосновать необходимость введения именно такой формулировки и таких признаков.

1. **Задание для студента 1:** Фокус на угрозе уничтожения, повреждения или блокирования компьютерной информации.
2. **Задание для студента 2:** Фокус на угрозе нарушения функционирования информационных систем.
3. **Задание для студента 3:** Фокус на массовом характере преступных действий или причинении крупного ущерба.
4. **Задание для студента 4:** Фокус на использовании вредоносных программ как способе совершения кибервымогательства.
5. **Задание для студента 5:** Фокус на кибервымогательстве, направленном на критическую информационную инфраструктуру.

Аудиторное занятие 3: Посягательства на криптовалюту и виртуальные вещи

Аудитория разделена на 3 станции. Учебная группа делится на 3 малых группы, в каждой группе – 3-5 человек. На станции № 1 группа работает с преподавателем (ответы обучающихся на вопросы преподавателя по изучаемой теме и групповая и (или) индивидуальная консультация). На станции № 2 группа самостоятельно выполняет одно общее практическое задание. На станции № 3 все члены группы выполняют индивидуальные, но однотипные задания. Задания на станциях разные. На данном практическом занятии все задания направлены на **понимание** основных положений темы;

анализ информации; **проведение оценки** и **получение нового опыта (разработка правовой позиции)**. Время работы группы на одной станции – **25 минут**. По истечении указанного времени группы переходят по часовой стрелке на следующую станцию для выполнения другого практического задания. В течение практического занятия каждая группа проходит все станции и выполняет все практические задания.

Вопросы для работы на станции № 1 с преподавателем (по содержанию темы, изученному дома самостоятельно с использованием предоставленного теоретического материала):

1. Объясните правовую природу "виртуальных вещей" (игровых артефактов, аккаунтов и т.п.). Являются ли они объектами гражданских прав? Можно ли их считать имуществом в контексте хищений?
2. Какие основные проблемы возникают при квалификации посягательств на виртуальные вещи? Приведите примеры из теоретического материала (дело Дмитрия Ш., случай в Красноярске).
3. Проанализируйте предложенный в теоретическом материале подход к квалификации принуждения к передаче виртуальных вещей через ст. 179 УК РФ. Насколько он, по вашему мнению, состоятелен? Каковы его ограничения?
4. Что такое криптовалюта? Каковы ее ключевые особенности с юридической точки зрения (децентрализация, отсутствие материальной формы, криптографическая защита)?
5. Проанализируйте дело Пирона и Пригожина. Какие выводы о правовом статусе криптовалюты как предмета преступления можно сделать на основе этого дела и позиции кассационного суда?
6. Какие аргументы "за" и "против" признания криптовалюты предметом хищения вы можете привести? Как текущая судебная практика и законодательство (включая Закон о ЦФА) влияют на этот вопрос?

Практическое задание для станции № 2 (общее).

Фабула: Группа лиц (Иванов, Петров, Сидоров) разработала план похищения дорогостоящих виртуальных предметов (уникальных "скинов" для оружия) в популярной онлайн-игре "CyberArena" у известного стримера "ProGamer". Для этого Иванов под видом фаната познакомился с "ProGamer" и, войдя в доверие, получил от него данные для входа в игровой аккаунт якобы для временного совместного использования редкого предмета. Получив доступ, Иванов передал данные Петрову, который специализировался на взломе. Петров, используя эти данные, вошел в аккаунт "ProGamer", изменил пароль и привязанный e-mail, а затем перевел все ценные виртуальные предметы на специально созданный аккаунт, контролируемый Сидоровым. Сидоров немедленно выставил эти предметы на продажу на "серой" интернет-площадке, где их приобрели третьи лица за реальные деньги, которые были перечислены на анонимный криптокошелек. Общая рыночная стоимость

похищенных виртуальных предметов на таких площадках оценивалась примерно в 300 000 рублей. "ProGamer" обратился в полицию.

Задание:

1. Проанализируйте действия Иванова, Петрова и Сидорова. Определите роль каждого в совершении предполагаемого деяния.
2. Оцените, можно ли квалифицировать их действия как хищение (например, по ст. 158, 159 или 159.6 УК РФ). Аргументируйте свою позицию, учитывая правовую природу виртуальных предметов и способы их получения/отчуждения.
3. Рассмотрите возможность квалификации содеянного по статьям главы 28 УК РФ (Преступления в сфере компьютерной информации), в частности ст. 272 УК РФ. Будет ли такая квалификация достаточной?
4. Предложите наиболее оптимальный, на ваш взгляд, вариант уголовно-правовой оценки действий группы лиц, исходя из действующего УК РФ и сложившейся (хотя и противоречивой) практики. Обоснуйте выбор и укажите на возможные проблемы доказывания и применения данной квалификации.
5. Как изменилась бы ситуация, если бы вместо виртуальных предметов были похищены биткоины с криптокошелька "ProGamer", доступ к которому был получен аналогичным образом?

Практические задания для станции № 3 (индивидуальные). Каждому студенту предлагается разработать краткую правовую позицию (основные тезисы) по одному из аспектов дела, описанного в задании для Станции №2, или по гипотетической ситуации с криптовалютой.

- **Студент 1 (Позиция обвинения по делу "ProGamer"):** Обосновать, почему действия группы лиц следует квалифицировать как хищение (выбрать конкретную форму) и/или преступление в сфере компьютерной информации, доказывая наличие всех признаков состава(ов).
- **Студент 2 (Позиция защиты по делу "ProGamer"):** Обосновать, почему действия группы лиц не образуют состава хищения (акцент на предмете) или почему квалификация по ст. 272 УК РФ является единственно возможной (или почему и она не применима).
- **Студент 3 (Позиция потерпевшего по делу о хищении криптовалюты):** Неизвестные получили доступ к его криптокошельку путем фишинга и перевели 5 ETH (эфириум) на другой адрес. Обосновать, почему криптовалюта должна признаваться имуществом и предметом хищения.
- **Студент 4 (Позиция следователя по делу о хищении криптовалюты из задания 3):** Сформулировать основные трудности, с которыми он столкнется при расследовании (установление личности преступника, доказывание умысла, определение размера ущерба, международный аспект).

- **Студент 5 (Аналитик-правовед):** Оценить перспективы признания виртуальных игровых предметов полноценными объектами гражданских прав и, соответственно, предметами хищения в РФ. Предложить возможные законодательные изменения.

Аудиторное занятие 4: Текущий контроль в форме подготовки мини-проекта по теме "Хищения с использованием новых информационных технологий"

Аудитория разделена на 3 станции. Учебная группа делится на 3 малых группы, в каждой группе – 3-5 человек. **Станция № 1 (Работа с преподавателем):** Обсуждение выбранных тем мини-проектов, уточнение целей, задач, структуры, методологии исследования, источников. Консультации по проблемным вопросам. **Станции № 2 и № 3 (Самостоятельная работа групп):** Студенты в малых группах (или индивидуально, если темы проектов индивидуальные) работают над своими мини-проектами: осуществляют поиск и анализ литературы и правоприменительной практики, формулируют основные положения проекта, разрабатывают структуру, готовят тезисы. Задания на станциях разные. На данном практическом занятии все задания направлены на **синтез** информации, **проведение оценки**, **получение нового опыта (разработка, проектирование)**. Время работы группы на одной станции – **25 минут** (преподаватель работает с каждой группой поочередно на Станции №1, пока другие группы работают самостоятельно на Станциях №2 и №3; затем группы могут поменяться для консультации или продолжить работу). Общее время работы над проектом в аудитории – 80 минут.

Задание: Подготовка мини-проекта по теме "Хищения с использованием новых информационных технологий"

Каждая малая группа (или студент индивидуально, по согласованию с преподавателем) выбирает одну из предложенных тем для мини-проекта. В течение аудиторного занятия студенты должны:

1. Определить цель и задачи своего проекта.
2. Составить предварительный план (структуру) проекта.
3. Подобрать и начать анализировать основные источники (нормативные акты, судебная практика, научные публикации).
4. Сформулировать ключевые тезисы и аргументы по выбранной теме.
5. Подготовить черновик введения и заключения (или основные идеи для них).

Окончательное оформление мини-проектов осуществляется студентами после занятия в рамках самостоятельной работы. Выполненный проект (в виде эссе, аналитической записки или презентации объемом 10-15 страниц/слайдов) направляется преподавателю в электронном виде в установленный срок. Контроль выполнения осуществляется дистанционно.

Методические рекомендации по выполнению заданий:

- **Общие:**
  - Внимательно читайте фабулу и вопросы к ней.
  - Используйте предоставленный теоретический материал, нормы УК РФ, Постановления Пленума ВС РФ.
  - Аргументируйте свою позицию, ссылаясь на конкретные признаки состава преступления (объект, объективная сторона, субъект, субъективная сторона).
  - При решении задач на квалификацию, рассматривайте все возможные варианты, объясняя, почему один из них является предпочтительным.
- **Для заданий Станции №1 (Работа с преподавателем):** Готовьтесь к дискуссии, формулируйте свои вопросы заранее, будьте готовы объяснить свою точку зрения.
- **Для заданий Станции №2 (Общее задание):** Работайте в команде, обсуждайте различные точки зрения, приходите к общему аргументированному решению. Распределяйте задачи внутри группы для эффективности.
- **Для заданий Станции №3 (Индивидуальные задания):**
  - При описании объективной стороны: четко указывайте действие (бездействие), способ, место, время, обстановку (если они имеют значение для квалификации), последствия, причинно-следственную связь.
  - При разработке предложений (например, по новой статье УК): стремитесь к юридической точности формулировок, учитывайте системность уголовного закона.
  - При разработке правовой позиции: будьте убедительны, используйте как нормативные аргументы, так и ссылки на доктрину или практику (если известна).
- **Для мини-проекта:**
  - Четко определите предмет, цель и задачи исследования.
  - Структурируйте материал логично (введение, основная часть с разделами/параграфами, заключение, список источников).
  - Критически анализируйте источники, не ограничивайтесь пересказом.
  - Формулируйте собственные выводы и предложения.
  - Соблюдайте требования к оформлению научных работ.

Примеры выполнения заданий (схематично):

- **Пример для Станции №2 (Занятие 1 - Мошенничество в сфере компьютерной информации):**
  - *Анализ действий Сидорова:* Сидоров, имея доступ, изменял реквизиты.
  - *Признаки ст. 159.6 УК РФ:*

        - Объект: отношения собственности ООО "ТехноСтрой".
        - Предмет: безналичные денежные средства.
        - Объективная сторона: хищение путем модификации (изменение реквизитов получателя) компьютерной информации (данных в бухгалтерской системе и платежных поручениях), что является вмешательством в функционирование средств обработки и передачи компьютерной информации. Последствия – причинение имущественного ущерба.
        - Субъект: специальный (лицо, использующее свое служебное положение – системный администратор).
        - Субъективная сторона: прямой умысел, корыстная цель.
    - *Отличие от иных статей:* Не ст. 158 (нет тайного изъятия), не ст. 159 (обман не физического лица, а воздействие на систему), не ст. 160 (имущество не было вверено Сидорову для управления).
    - *Характеристика действий:* Изменение реквизитов – модификация. Доступ и изменение – вмешательство.
- **Пример для Станции №3 (Занятие 2 - Кибервымогательство, индивидуальное задание - разработка диспозиции):**
    - *Студент 1 (Фокус на угрозе уничтожения, повреждения или блокирования):*
        - "Кибервымогательство, то есть требование передачи чужого имущества, права на имущество или совершения других действий имущественного характера под угрозой уничтожения, повреждения, блокирования компьютерной информации либо нарушения нормального функционирования компьютерной системы или сети, – наказывается..."
        - Квалифицирующие признаки: 1) совершенное группой лиц по предварительному сговору; 2) с причинением крупного ущерба.
        - Обоснование: Данная формулировка охватывает специфику угрозы в цифровой среде, а квалифицирующие признаки отражают повышенную опасность.
- **Пример выполнения мини-проекта (схематично, по теме "Проблемы квалификации хищений денежных средств с банковских счетов...")**
    - **Цель:** Выявить критерии разграничения и проблемы конкуренции ст. 158 п. "г" ч.3, ст. 159.3 и ст. 159.6 УК РФ.
    - **Задачи:**

1. Анализ легальных определений и признаков составов.
2. Изучение ППВС РФ от 30.11.2017 № 48 и других релевантрых актов.

3. Анализ 15-20 приговоров судов по данным статьям для выявления подходов к квалификации.
4. Выявление типичных ошибок и спорных ситуаций.
5. Формулировка предложений по оптимизации правоприменения.

- **Структура:**
  - Введение (актуальность, цель, задачи, методы).
  - Глава 1. Теоретико-правовой анализ составов преступлений (ст. 158 п."г" ч.3, 159.3, 159.6 УК РФ): объект, предмет, объективная сторона (особенно способ).
  - Глава 2. Проблемы правоприменения и разграничения смежных составов:
    - 2.1. Анализ судебной практики: ключевые подходы и противоречия.
    - 2.2. Разграничение кражи с банковского счета и мошенничества с использованием электронных средств платежа.
    - 2.3. Разграничение мошенничества с использованием ЭСП и мошенничества в сфере компьютерной информации.
  - Глава 3. Предложения по совершенствованию законодательства и правоприменительной практики (если необходимо) или научно-обоснованные критерии разграничения.
  - Заключение (основные выводы).
  - Список использованных источников.
- **Ожидаемые выводы (пример):** Ключевым критерием разграничения ст. 159.3 и 159.6 является характер воздействия: в первом случае – обман уполномоченного работника или использование заранее похищенных/поддельных карт, во втором – непосредственное вмешательство в работу компьютерных систем. Разграничение со ст. 158 п. "г" ч.3 зависит от наличия/отсутствия обмана или вмешательства, определяющих способ хищения как мошеннический или тайный.

3. Проверка практических заданий, выполненных обучающимися:

Проверка заданий, выполненных на станциях №2 и №3, осуществляется преподавателем после занятия. На следующем занятии выборочно разбираются наиболее интересные или типичные случаи, а также допущенные ошибки. Особое внимание уделяется аргументации студентов и пониманию ими ключевых различий между составами преступлений. Мини-проекты проверяются преподавателем дистанционно после их сдачи. Предоставляется индивидуальная обратная связь каждому студенту/группе.

Шкала и критерии оценивания выполненных заданий:

Оценка производится по классической 5-балльной шкале.

- **"Отлично" (5 баллов):**
  - Задания на станциях: Дан полный, развернутый ответ на все поставленные вопросы. Продемонстрировано глубокое понимание материала, способность к анализу и синтезу. Квалификация предложена верно, исчерпывающе аргументирована со ссылками на НПА и теорию. Предложения по совершенствованию законодательства (если требовалось) оригинальны, юридически грамотны и обоснованы.
  - Мини-проект: Соответствует всем индикаторам компетенций. Исследование глубокое, всестороннее. Выводы оригинальны, аргументированы. Использован широкий круг источников. Оформление безупречно.
- **"Хорошо" (4 балла):**
  - Задания на станциях: Ответы в целом верные и полные, но могут содержать незначительные неточности или недостаточно глубокую аргументацию по отдельным аспектам. Квалификация в целом верна, но могут быть упущения в обосновании.
  - Мини-проект: В целом соответствует индикаторам. Исследование проведено на достаточном уровне, но некоторые аспекты могли бы быть раскрыты глубже. Выводы в основном верны, но могут быть недостаточно оригинальны или аргументированы. Есть незначительные замечания по оформлению или использованию источников.
- **"Удовлетворительно" (3 балла):**
  - Задания на станциях: Продемонстрировано общее понимание темы, но допущены существенные ошибки в ответах или квалификации. Аргументация слабая или отсутствует по некоторым пунктам. Понимание ключевых различий между составами поверхностное.
  - Мини-проект: Частично соответствует индикаторам. Исследование поверхностное, либо раскрыта только часть темы. Выводы не всегда аргументированы или основаны на ограниченном количестве источников. Имеются существенные замечания по содержанию и/или оформлению.
- **"Неудовлетворительно" (2 балла):**
  - Задания на станциях: Ответы неверные, либо демонстрируют полное непонимание темы. Квалификация неверна или отсутствует.
  - Мини-проект: Не соответствует индикаторам компетенций. Тема не раскрыта. Отсутствует анализ, выводы не обоснованы. Работа носит реферативный характер или содержит плагиат.

Задания для самостоятельной работы по теме "Хищения с использованием новых информационных технологий":

1. Изучить Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 "О судебной практике по делам о мошенничестве, присвоении и растрате" (в части, касающейся ст. 159.3, 159.6 УК РФ). Подготовить краткий конспект основных разъяснений.
2. Найти и проанализировать 3-5 обвинительных приговоров по ст. 159.6 УК РФ, обратив внимание на описание способа совершения преступления и доказательственную базу.
3. Подготовить эссе на тему: "Проблемы определения момента окончания мошенничества в сфере компьютерной информации".
4. Изучить научные статьи (2-3) по проблемам уголовно-правовой оценки кибервымогательства. Составить аннотации.
5. Проанализировать зарубежное законодательство (на примере 1-2 стран) об ответственности за посягательства на криптовалюту или виртуальное игровое имущество.
6. Подготовить сравнительную таблицу признаков составов преступлений, предусмотренных ст. 158 (п. "г" ч. 3), ст. 159, ст. 159.3, ст. 159.6, ст. 163, ст. 272 УК РФ, применительно к хищениям с использованием информационных технологий.

Список вопросов для самоконтроля:

1. В чем специфика предмета преступления, предусмотренного ст. 159.6 УК РФ?
2. Какие действия охватываются понятием "вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации"?
3. Как разграничить мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и кражу с банковского счета (п. "г" ч. 3 ст. 158 УК РФ)?
4. Каковы основные способы совершения кибервымогательства?
5. С какими трудностями сталкивается правоприменитель при квалификации кибервымогательства по действующему УК РФ?
6. Почему "классическая" ст. 163 УК РФ не всегда применима к случаям кибервымогательства?
7. Каков правовой статус виртуальных вещей (игровых ценностей) в российском праве? Могут ли они быть предметом хищения?
8. Какие аргументы существуют "за" и "против" признания криптовалюты имуществом и, соответственно, предметом хищения?
9. Какова позиция Верховного Суда РФ (и нижестоящих судов, если известна из практики) по вопросу о криптовалюте как предмете преступного посягательства?
10. Какие нормы УК РФ, помимо статей о хищениях, могут применяться при посягательствах на криптовалюту и виртуальные ценности?

4. Текущий контроль успеваемости по теме № 3

Текущий контроль успеваемости проводится в форме выполнения мини-проекта.

Шкала и критерии оценивания приведены в оценочных средствах по дисциплине «Преступления в сфере высоких технологий» для данной ОПОП ВО, которые размещены на официальном сайте университета по ссылке https://swsu.ru/sveden/education/eduop/.

ТЕМА № 4
ПРЕСТУПЛЕНИЯ ПРОТИВ ЛИЧНОСТИ, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

I. ДИСТАНЦИОННАЯ ЧАСТЬ

Задания, выполняемые до начала первого практического занятия по теме № 4

Внеаудиторная (домашняя) самостоятельная работа обучающихся по освоению основных положений темы № 4: предварительное (до начала первого практического занятия по теме) самостоятельное изучение теоретического учебного контента по новой теме дисциплины, разработанного преподавателем и представленного в цифровом формате на портале do.swsu.ru

1.1 Ознакомьтесь с **инструкцией** о порядке организации самостоятельной работы по изучению данной темы и следуйте ей.

1.2. Прочитайте **перечень основных теоретических вопросов**, которые необходимо самостоятельно освоить, и **текст с изложением указанных вопросов**.

1.3 Работая с текстом, вносите по мере чтения необходимые записи в **опорный конспект**, который поможет вам запомнить главное.

Опорный конспект по теме № 4 «Преступления против личности, совершаемые с применением информационных технологий»

1. ЗАПОМИНАЕМ ГЛАВНОЕ

1.1 Впишите пропущенные слова/словосочетания:

а) Преступления против личности, предполагающие возможность _____ воздействия на потерпевшего, могут совершаться с использованием ИТС.

б) «Переход в реал» – это ситуация, когда межличностный конфликт, возникший в _____, заканчивается _____ действиями в «реальном мире».

в) «Группы смерти» – это условное наименование сообществ, якобы вовлекающих подростков в смертельную игру, последним шагом в которой должно стать _____. Публикация о них в «Новой газете» вызвала явление, известное как _____.

г) Статья 110.1 УК РФ предусматривает ответственность за склонение к совершению самоубийства или _____ совершению самоубийства путем _____ , _____ или иным способом, при отсутствии признаков доведения до самоубийства. Состав преступления – _____.

д) Статья 110.2 УК РФ устанавливает ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства путем _____ информации о способах совершения самоубийства или _____ к совершению самоубийства.

е) КИБЕРБУЛЛИНГ – это психологическая _____ с использованием механизмов _____ коммуникаций.

ж) СТАЛКИНГ – это _____ преследование, а КИБЕРСТАЛКИНГ – его разновидность с использованием _____.

з) ГРУМИНГ – это долговременное установление взрослым _____, _____ отношений с ребенком с целью завоевания _____ и последующего _____.

и) ДОКСИНГ – это совершённые онлайн поиск и публикация _____ или _____ информации о человеке без его _____, обычно с целью _____, _____ или _____.

к) СВАТТИНГ – это тактика сталкинга, заключающаяся во введении _____ в заблуждение так, чтобы по адресу другого лица выехала _____ группа.

1.2 Заполните пропуски, связанные с хронологией и особенностями "групп смерти", и установите соответствия:

А) Хронология и факты:

* Статья Г. Мурсалиевой «Группы смерти» в «Новой газете» появилась _____ (дата).

* Самоубийство школьницы, известной как Рина Паленкова, произошло _____ (дата).

* Участникам «игры» якобы давалось _____ дней на принятие решения о самоубийстве.

* Символами культа «групп смерти» являлись изображения _____ и _____.

Б) Установите соответствие между статьей УК РФ и ее основным содержанием:

Статья УК РФ	**Содержание**
1. Ст. 110	А) Клевета
2. Ст. 110.1	Б) Истязание
3. Ст. 110.2	В) Нарушение неприкосновенности частной жизни
4. Ст. 117	Г) Доведение до самоубийства (путем угроз, жестокого обращения или систематического унижения)
5. Ст. 119	Д) Склонение к совершению самоубийства или содействие совершению самоубийства
6. Ст. 128.1	Е) Организация деятельности, направленной на побуждение к совершению самоубийства
7. Ст. 137	Ж) Угроза убийством или причинением тяжкого вреда здоровью

1.3 Укажите стрелочкой одно наиболее точное соответствие:

КИБЕРБУЛЛИНГ -->

Любой конфликт в сети Интернет

Распространение вредоносных программ

Агрессивное преследование и издевательство над одним из членов коллектива с использованием электронных коммуникаций

Законное выражение своего мнения в онлайн-дискуссии

Мошенничество с использованием банковских карт онлайн

1.4 Запишите наименования:

А) Формы кибербуллинга:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Б) Особенности кибербуллинга, отличающие его от традиционного буллинга:

1. _____
2. _____
3. _____

В) Возможные направления совершенствования законодательства в сфере противодействия кибersталкингу и кибербуллингу (по тексту лекции):

1. Включение в ст. 110 УК РФ указания на _____ как на способ доведения до самоубийства.
2. Включение в ст. 117 УК РФ указания на _____ как способ причинения психических страданий.
3. Включение в ст. 119 УК РФ указания на то, что ответственность наступает, если угрозы совершаются с использованием ИТ и носят _____ характер.
4. Включение в ст. 306 УК РФ _____ как самостоятельной формы преступного деяния.

2. АНАЛИЗИРУЕМ ПРАКТИКУ И ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ

2.1 Кратко опишите примеры преступлений (или ситуаций, требующих правовой оценки) из текста лекции, связанных с использованием ИТ:

№	Описание ситуации (фабула)	Задействованные ИТ / Суть использования ИТ	Возможная правовая квалификация / Проблема
1	Убийство в Волгограде (2020 г.)	Ссора в _____	Преступление в "реале" после конфликта в ИТС.
2	Деятельность "групп смерти" (случай Рины Паленковой)	Социальная сеть «Вконтакте», чаты, ARG (игры в альтернативной реальности)	Ст. _____, ст. _____ УК РФ. Проблема _____ паники.
3	Деанонимизация порноактрис пользователями «Двача» с помощью сервиса FindFace	Сервис _____, социальная сеть «ВКонтакте», имиджборд «Двач»	Ст. _____ УК РФ (клевета), ст. _____ УК РФ (нарушение неприкосновенности частной жизни). Мотивация: _____

4	"Клеветническая порноместь"	Создание страниц в _____, размещение _____ информации и фото-/видеомонтажа.	Совокупность ст. _____ и ст. _____ УК РФ, или только ст. _____ УК РФ. Возможна ст. _____ УК РФ.
5	Виртуальное изнасилование аватара в игре Horizon Worlds	VR-шлем, виртуальный мир игры, _____ контроллера.	Проблема _____ такого деяния по действующему УК РФ.
6	Сваттинг (пример не из РФ, но суть явления)	Введение _____ в заблуждение для выезда штурмовой группы.	Отсутствие специальной нормы в УК РФ. Предложение: в _____ УК РФ.

3.1 Сформулируйте кратко вывод, который Вы сделали лично для себя после изучения темы «Преступления против личности, совершаемые с применением информационных технологий»:

1.4 Посмотрите **видеоролик** по теме № 4 в ходе чтения текста (параллельно с ним).

Обратите внимание на то, что для противодействия «группам смерти» в УК РФ были введены две новых статьи: ст. 110.1 и 110.2 УК РФ, предусматривающие ответственность за склонение и содействие в совершении самоубийства, а также за организацию деятельности, направленной на побуждение к самоубийству.

1.5 Перескажите изученный теоретический материал по вопросам, указанным в инструкции, и опорному конспекту. Воспользуйтесь также следующими **вопросами для самоконтроля**:

1. Какие преступления против личности наиболее подвержены цифровой трансформации? Приведите примеры.
2. В чем заключается опасность "групп смерти" и какие статьи УК РФ направлены на противодействие им?
3. Охарактеризуйте составы преступлений, предусмотренные ст. 110.1 и 110.2 УК РФ. В чем их различие?
4. Что такое кибербуллинг и каковы его основные формы?
5. Чем кибербуллинг отличается от обычного буллинга?
6. Что такое киберсталкинг и каковы его особенности?
7. Что такое троллинг и как он может быть связан с персонифицированным сталкингом?
8. Какие формы кибербуллинга, киберсталкинга и троллинга представляют наибольшую опасность?
9. Какие существуют проблемы правоприменения в отношении кибербуллинга и киберсталкинга?

10. Какие изменения в УК РФ предлагаются для более эффективного противодействия кибербуллингу и киберсталкингу?
11. Что такое "клеветническая порноместь" и как она квалифицируется?
12. Какие половые преступления чаще всего совершаются с использованием ИТС?
13. Что такое груминг и каковы его признаки?
14. Какие цели преследует грумер?
15. Какие формы виртуального домогательства существуют?
16. Что такое доксинг и каковы его цели?
17. Что такое порноместь и какие последствия она может повлечь?
18. Каковы причины массовых утечек персональных данных пользователей онлайн-сервисов?
19. Какие вопросы, связанные с тайной переписки в интернете, остаются слабо урегулированными?
20. Какие проблемы возникают при привлечении к ответственности за неправомерное вмешательство в электронное голосование?
21. В чем заключается проблема вовлечения несовершеннолетних в противоправную деятельность через интернет-сообщества?
22. Какие изменения в законодательстве предлагаются для решения проблемы вовлечения несовершеннолетних в противоправную деятельность через интернет-сообщества?

1.6 Возьмите с собой на практическое занятие свой **опорный конспект** по теме № 4.

1.7 Выполните **входное тестирование** по теме № 4.

Ответьте на вопросы и выполните задания в тестовой форме по теме № 4:

Вопросы в закрытой форме:

1. Укажите, какая статья Уголовного кодекса РФ была введена, в частности, для противодействия деятельности так называемых «групп смерти»: а) ст. 110 УК РФ «Доведение до самоубийства» б) ст. 111 УК РФ «Умышленное причинение тяжкого вреда здоровью» в) ст. 110.1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства» г) ст. 128.1 УК РФ «Клевета» д) ст. 151.2 УК РФ «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего»
2. Согласно тексту лекции, какой основной мотив преследователей в примере с использованием сервиса FindFace для деанонимизации порноактрис на имиджборде «Двач»? а) Получение материальной выгоды б) Осуществление научной деятельности в) Восприятие жертв как «продажных и обманчивых», желание их «разоблачить» г) Защита общественной нравственности д) Выполнение заказа от конкурентов жертв

3. Какая из перечисленных особенностей НЕ характерна для кибербуллинга, согласно представленному материалу? а) Отсутствие географических и временных ограничений б) Широта аудитории в) Анонимность преследователя г) Обязательное наличие тесного физического контакта между преследователем и жертвой д) Возможность вовлечения посторонних лиц в травлю
4. Какая проблема правоприменения ст. 119 УК РФ («Угроза убийством или причинением тяжкого вреда здоровью») особенно актуальна в контексте анонимных угроз через Интернет? а) Сложность определения размера причиненного морального вреда б) Трудность доказывания наличия оснований опасаться реального осуществления угрозы в) Отсутствие в статье указания на информационные технологии как способ совершения преступления г) Необходимость установления прямого умысла на доведение до самоубийства д) Отсутствие потерпевшего как такового
5. В каком случае, согласно тексту, развратные действия с лицом, не достигшим 12-летнего возраста, совершенные с использованием ИТС, будут квалифицироваться по ст. 132 УК РФ? а) Только если они сопровождались физическим насилием б) Если они повлекли заражение венерическим заболеванием в) В любом случае, так как возраст потерпевшего определяет квалификацию по данной статье для таких действий г) Только если они были совершены группой лиц по предварительному сговору д) Если они были направлены на изготовление детской порнографии
6. Какая основная причина, согласно тексту, появления массовых «сливов» персональных данных пользователей онлайн-сервисов? а) Целенаправленные действия иностранных спецслужб б) Недостатки в обеспечении информационной безопасности операторов сервисов в) Массовое использование пользователями слабых паролей г) Глобальные сбои в работе сети Интернет д) Отсутствие законодательного регулирования обработки персональных данных
7. Какая цель, согласно тексту, преследовалась при массовом взломе учётных записей сайта «Госуслуги» в 2021 году? а) Получение доступа к финансовым средствам граждан б) Шантаж государственных органов в) Влияние на «праймериз» одной из политических партий г) Тестирование уязвимостей системы д) Сбор данных для социологического исследования
8. Почему, согласно тексту, несовершеннолетние представляют собой привлекательную аудиторию для администраторов сообществ, вовлекающих в противоправную деятельность? а) Они обладают большими финансовыми ресурсами б) Они лучше разбираются в информационных технологиях в) Они легче поддаются внушению, ими легче манипулировать, и они не в полной мере оценивают риски г) Они

чаще ищут способы заработка в интернете д) Они более склонны к анонимности в сети

Вопросы в открытой форме:

9. Тактика сталкинга, которая заключается во введении полиции в заблуждение так, чтобы по адресу другого лица выехала штурмовая полицейская группа путем фальшивых сообщений о серьёзных правонарушениях, называется _____.
10. Совершённые онлайн поиск и публикация персональной или конфиденциальной информации о человеке без его согласия, обычно с целью шантажировать жертву, отомстить ей или затравить её, – это _____.
11. Возбуждение желания совершить самоубийство при отсутствии признаков доведения до самоубийства, где способ склонения может быть любым, кроме связанных с угрозами, насилием, систематическим унижением человеческого достоинства, и должно быть направлено на конкретное лицо, в УК РФ определяется как _____.
12. Агрессивное преследование и издевательство над одним из членов коллектива со стороны другого или группы лиц, при котором жертва оказывается не в состоянии защитить себя от нападок, в психологической форме с использованием механизмов электронных коммуникаций, называется _____.
13. Долговременное установление взрослым близких, доверительных отношений с ребенком с целью завоевания доверия и последующего совращения, часто с использованием онлайн-платформ, называется _____.
14. Размещение в ИТС фотографий и видеозаписей интимного характера, на которых действительно запечатлена жертва, с целью отомстить или досадить ей, при этом съемка могла осуществляться с согласия жертвы или самой жертвой, именуется в тексте как «классическая» _____.
15. Согласно тексту, одним из предложений по совершенствованию законодательства в сфере борьбы с клеветой в интернете является установление _____ порядка производства по делам о квалифицированном составе клеветы с использованием информационных технологий и ИТС, чтобы обеспечить выявление виновного силами правоохранительных органов.
16. Распространение информации о способах совершения самоубийства или не направленных на конкретное лицо призывов к самоубийству само по себе _____, однако организация деятельности, направленной на побуждение к совершению самоубийства путем такого распространения или призывов, является уголовно наказуемой.

Вопросы на установление правильной последовательности:

17. Расположите в хронологическом порядке события, связанные с феноменом «групп смерти», как они описаны в тексте:
    1. Публикация статьи Г. Мурсалиевой «Группы смерти» в «Новой газете»
    2. Появление фотографий Рины Паленковой (Ренаты Камболиной) после самоубийства и распространение мемов
    3. Анонсирование администраторами группы «f57» так называемого «флешмоба самоубийств»
    4. Запуск интерактивного квеста ARG на основе задумки «Инсайдер»
18. Расположите в примерной последовательности этапы (тактики) груминга, как они могут быть выведены из описания в тексте:
    1. Изоляция жертвы от окружающих, создание недоверия к родителям
    2. Установление доверительных отношений, имитация дружбы или любви, возможная помощь
    3. Нормализация физического контакта (если применимо к онлайн-переходу в офлайн) или интимного общения онлайн, проламывание границ
    4. Шантаж или использование чувства долга/вины для сексуальной эксплуатации
19. Восстановите логическую последовательность действий при совершении так называемой «клеветнической порномести», согласно описанию в тексте:
    1. Размещение на созданных страницах заведомо ложной информации об интимных предпочтениях потерпевших и фотоиллюстраций
    2. Разрыв отношений между злоумышленником (чаще мужчиной) и потерпевшей (девушкой)
    3. Создание от имени потерпевших страниц в социальных сетях
    4. Возможная квалификация действий по ст. 128.1 УК РФ и/или ст. 137 УК РФ

Вопросы на установление соответствия:

20. Установите соответствие между статьей УК РФ и ее основным содержанием, упомянутым в контексте преступлений с использованием ИТ: А) Ст. 110.1 УК РФ Б) Ст. 110.2 УК РФ В) Ст. 128.1 УК РФ Г) Ст. 137 УК РФ
    1. Клевета
    2. Нарушение неприкосновенности частной жизни
    3. Склонение к совершению самоубийства или содействие совершению самоубийства
    4. Организация деятельности, направленной на побуждение к совершению самоубийства

21. Установите соответствие между формой кибербуллинга (согласно тексту) и ее кратким описанием: А) Очернение и распространение слухов Б) «Кража личности» В) Социальная изоляция Г) Домогательство
    1. Использование чужих аккаунтов или создание фейковых страниц от имени жертвы
    2. Систематические оскорбительные сообщения, часто сексуального характера
    3. Исключение жертвы из онлайн-групп, игнорирование в чатах
    4. Публикация ложной порочащей информации о жертве
22. Установите соответствие между проблемой правоприменения существующей нормы УК РФ и предлагаемым в тексте направлением ее регулирования: А) Ст. 110 УК РФ (Доведение до самоубийства) не охватывает шантаж как способ. Б) Ст. 117 УК РФ (Истязание) указывает на насильственный характер действий, причиняющих психические страдания, что затрудняет применение к онлайн-преследованию. В) Ст. 306 УК РФ (Заведомо ложный донос) не охватывает специфику сваттинга. Г) Ст. 128.1 УК РФ (Клевета) по делам частного обвинения создает трудности при анонимном распространении в сети.
    1. Включить указание на анонимную или систематическую отправку электронных сообщений как способ причинения психических страданий.
    2. Установить, что производство по квалифицированному составу клеветы с использованием ИТС осуществляется в частно-публичном порядке.
    3. Включить указание на шантаж как на способ доведения до самоубийства.
    4. Включить сваттинг как самостоятельную форму преступного деяния.
23. Установите соответствие между термином, обозначающим деструктивное онлайн-поведение, и его ключевой характеристикой из текста: А) Троллинг Б) Сваттинг В) Доксинг Г) Груминг
    1. Введение полиции в заблуждение для выезда штурмовой группы по адресу жертвы.
    2. Установление доверительных отношений с ребенком с целью последующего совращения.
    3. Форма социальной провокации или издевательства в сетевом общении для эпатажа или разжигания конфликтов.
    4. Поиск и публикация персональной информации о человеке без его согласия с целью шантажа или травли.
24. Установите соответствие между видом преступного деяния с использованием ИТ и его возможным проявлением, описанным в тексте: А) «Клеветническая порноместь» Б) Кибersталкинг В) Вовлечение

несовершеннолетних в опасные действия через онлайн-сообщества Г) Нарушение тайны переписки

1. Использование взломанных учётных записей для доступа к сообщениям в мессенджерах.
2. Создание фейковых аккаунтов от имени бывшей партнерши с размещением ложной информации о предложении ею сексуальных услуг.
3. Координация нелегальных уличных гонок через закрытые группы в социальных сетях.
4. Навязчивое преследование с угрозами и оскорблениями в социальных сетях, осуществляемое анонимно в течение длительного времени.

25. Установите соответствие между предлагаемым направлением регулирования в сфере половых преступлений с использованием ИТ и его сутью: А) Криминализация отдельных форм виртуального домогательства Б) Устранение пробелов в криминализации груминга В) Правовая регламентация оперативно-розыскных мероприятий Г) Учет покушения на негодный объект при развратных действиях
    1. Чёткое указание, что преступным является покушение, когда переписку от имени несовершеннолетнего ведут взрослые (родители, правоохранители).
    2. Установление ответственности за подстрекательство лица, не достигшего 16-летнего возраста, к встрече с целью сексуальных отношений.
    3. Включение в состав ст. 133 УК РФ побуждения к созданию материалов с изображением действий сексуального характера (секстинг).
    4. Разработка правил для правоохранительных органов по выявлению «грумеров» в сети.

II. АУДИТОРНАЯ ЧАСТЬ

Практическое занятие № 4
«Преступления против личности, совершаемые с применением информационных технологий»

Цель практического занятия – приобретение обучающимися практического опыта в применении знаний, полученных при самостоятельном освоении темы № 4, в производственных ситуациях.

Планируемые результаты обучения:

Знать:	**Уметь:**	**Иметь опыт**

		деятельности:
содержание норм, устанавливающих ответственность за преступные деяния, связанные с преступлениями в сфере высоких технологий, особенности их реализации; методологические основы реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; содержание постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, связанных с уголовно-правовым регулированием ответственности за преступления в сфере высоких технологий; особенности оценки на соответствие признакам преступления (квалификации) конкретных преступлений в сфере высоких технологий,	использовать информацию о нормах, устанавливающих ответственность за преступления в сфере высоких технологий, в целях их реализации; применять нормы особенной части уголовного права, регулирующие ответственность за преступления в сфере высоких технологий; применять нормы особенной части уголовного права, регулирующие ответственность за преступления в сфере высоких технологий с учётом постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований; давать полную и точную квалификацию преступлений в сфере высоких технологий, с учётом положений Общей и Особенной части уголовного законодательства, разъяснений Пленума Верховного Суда РФ; толковать положения актов уголовного	по обобщению и анализу информации, имеющей значение для реализации правовых норм в сфере установления ответственности за преступления в сфере высоких технологий; по реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по обобщению и анализу постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, касающихся норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по принятию решений, связанных с оценкой на соответствие конкретных деяний, связанных с высокими технологиями,

предусмотренных уголовным законодательством; способы толкования норм уголовного законодательства, позволяющие вычленить из их текста основные юридически значимые признаки преступных деяний, связанных с высокими технологиями, и сопоставить их с признаками преступления; особенности толкования норм уголовного законодательства, устанавливающих ответственность за конкретные преступления в сфере высоких технологий, позволяющие разграничить между собой смежные составы преступлений при наличии конкуренции норм	законодательства, касающиеся высоких технологий, основываясь на общих принципах толкования нормативных актов; разъяснять содержание норм уголовного законодательства, предусматривающих ответственность за совершение конкретных преступлений в сфере высоких технологий, с учётом судебной практики и доктрины уголовного права; устанавливать содержание оценочных признаков норм уголовного законодательства, регулирующих ответственность за преступления в сфере высоких технологий, а также признаков, позволяющих разграничить между собой смежные преступные деяния при наличии конкуренции норм	признакам преступления; по применению основных подходов к толкованию норм уголовного законодательства Российской Федерации, касающихся высоких технологий, и вычленению признаков конкретного деяния; по выявлению точного содержания норм уголовного законодательства, устанавливающих общие условия уголовной ответственности и освобождения от неё, а также признаки конкретных составов преступлений, связанных с преступлениями в сфере высоких технологий; по применению приёмов научного мышления, позволяющих устанавливать смысл нормоустановлений уголовно-правового характера, касающихся высоких технологий, в условиях правовой неопределённости, коллизий правового регулирования, конкуренции норм

Необходимое материально–техническое оборудование: ноутбук и (или) мобильные устройства преподавателя и обучающихся.

ПЛАН ПРАКТИЧЕСКОГО ЗАНЯТИЯ № 4

1. Уточнение и (или) углубление отдельных вопросов по теме № 4.
2. Выполнение обучающимися практических заданий.
3. Проверка практических заданий, выполненных обучающимися.
4. Текущий контроль успеваемости по теме № 4

1. Уточнение и (или) углубление отдельных вопросов по теме № 4

Консультация преподавателя

Студенты методом мозгового штурма формируют перечень вопросов, которые при самостоятельном освоении темы дома или при тестировании остались для них непонятными или показались сложными и (или) спорными. Преподаватель по результатам тестирования при необходимости добавляет в сформированный обучающимися список вопросы, которые, с его точки зрения, требуется уточнить или углубить.

Определяя с помощью поднятых рук количество студентов, считающих сложным конкретный вопрос из сформированного списка, преподаватель устанавливает вопросы, по которым сразу же проводит групповую консультацию.

Если в пояснениях нуждаются 1-2 человека, преподаватель индивидуально консультирует их в ходе практического занятия.

2. Выполнение обучающимися практических заданий

На данном практическом занятии выполнение обучающимися практических заданий проводится по технологии метода анализа конкретных ситуаций (кейс-стади) с элементами проектной деятельности и групповой дискуссии.

ПЕРЕЧЕНЬ ВЫПОЛНЯЕМЫХ ЗАДАНИЙ

Аудиторное занятие 1: Деяния, связанные с суицидом

1. **Уровень "Понимание" (20 минут):**
    - **Задание 1.1.** Используя текст Уголовного кодекса РФ (ст. 110, 110.1, 110.2) и предоставленный теоретический материал, дайте устное определение понятиям: "доведение до самоубийства", "склонение к совершению самоубийства или содействие совершению самоубийства", "организация деятельности, направленной на побуждение к совершению самоубийства". Объясните своими словами ключевые различия между этими составами преступлений. Обсудите в группе, какие именно действия в сети Интернет могут подпадать под признаки "склонения", а какие – под "содействие".

2. **Уровень "Применение" (30 минут):**
   - **Задание 1.2.** Проанализируйте следующую гипотетическую ситуацию: *Гражданин П., администратор закрытого онлайн-сообщества, на протяжении месяца вел переписку с 15-летней К., испытывавшей психологические трудности. П. убеждал К. в бессмысленности ее существования, описывал различные способы ухода из жизни как "красивый и смелый поступок", давал советы по выбору "наименее болезненного способа", а также направил ей ссылку на интернет-ресурс, где подробно описывались летальные дозировки определенных медицинских препаратов. В результате К. совершила покушение на самоубийство, но была спасена. Квалифицируйте действия гражданина П. Обоснуйте свой ответ, указав на конкретные признаки состава (составов) преступления.*
3. **Уровень "Анализ" (30 минут):**
   - **Задание 1.3.** На основе теоретического материала ("Группы смерти", "Факты", "Вопрос реальности") и дополнительного поиска (при необходимости, под руководством преподавателя) сравните феномены так называемых "групп смерти" и ARG (игр в альтернативной реальности) с суицидальной тематикой. Выделите общие черты и принципиальные различия. Проанализируйте, в чем заключается реальная опасность таких сообществ для подростков, даже если их организаторы не ставят прямой цели доведения до самоубийства.

Аудиторное занятие 2: Травля и клевета

1. **Уровень "Понимание" (20 минут):**
   - **Задание 2.1.** Используя теоретический материал ("Кибербуллинг", "Сталкинг", "Троллинг", "Клевета"), дайте определения этим явлениям. Обсудите в малых группах (3-4 человека) специфические особенности кибербуллинга, отличающие его от традиционной травли. Каждая группа представляет 2-3 ключевых отличия.
2. **Уровень "Применение" (30 минут):**
   - **Задание 2.2.** *Гражданка С. после расставания с гражданином Л. стала объектом преследования в социальной сети. Л. создал несколько фейковых аккаунтов, с которых отправлял С. оскорбительные сообщения, угрозы распространить ее личные фотографии, а также публиковал на ее странице (в комментариях к ее постам) ложную информацию о том, что С. якобы оказывает интимные услуги за деньги. Кроме того, Л. отправил аналогичные сообщения нескольким друзьям и коллегам С. Дайте предварительную правовую оценку действиям Л. Какие*

статьи УК РФ могут быть применимы? Какие трудности в доказывании могут возникнуть?

3. **Уровень "Анализ" и "Синтез" (30 минут):**
    - **Задание 2.3.** Проанализируйте текущие проблемы правоприменения в случаях кибersталкинга и кибербуллинга, описанные в теоретическом материале ("Проблемы правоприменения"). Работая в малых группах, разработайте и представьте предложения по внесению изменений в действующее уголовное законодательство РФ, направленные на криминализацию наиболее опасных форм кибersталкинга, не охватываемых существующими нормами. Обоснуйте необходимость предлагаемых изменений.

Аудиторное занятие 3: Половые преступления. Иные преступления против личности

1. **Уровень "Понимание" и "Применение" (30 минут):**
    - **Задание 3.1.** Ознакомьтесь с понятиями "груминг", "порноместь", "доксинг" в теоретическом материале. *Приведите по одному гипотетическому примеру для каждого из этих деяний, совершаемых с использованием ИТ. Для каждого примера укажите, под признаки каких статей УК РФ (если таковые имеются) могут подпадать описанные действия. Обсудите, всегда ли существующие нормы УК РФ адекватно охватывают общественную опасность этих деяний.*
2. **Уровень "Анализ" (25 минут):**
    - **Задание 3.2.** Изучите раздел теоретического материала "Виртуальное изнасилование?". Проанализируйте, существуют ли в действующем российском уголовном законодательстве нормы, позволяющие привлечь к ответственности за подобные действия в виртуальной среде. Аргументируйте свою позицию. Сравните с подходами, существующими (или обсуждаемыми) в зарубежных правовых системах (если информация доступна или будет предоставлена преподавателем).
3. **Уровень "Синтез" и "Получение нового опыта" (25 минут):**
    - **Задание 3.3.** На основе раздела "Направления регулирования" (касающегося половых преступлений, доксинга, порномести) и собственных суждений, предложите 1-2 конкретные законодательные инициативы (в форме тезисов или кратких формулировок предполагаемых норм/изменений в нормы), направленные на повышение эффективности противодействия этим преступлениям. Кратко обоснуйте целесообразность ваших предложений.

Аудиторное занятие 4: Текущий контроль в форме подготовки разбора конкретной ситуации по теме "Преступления против личности, совершаемые с применением информационных технологий"

- **Уровни "Анализ", "Синтез", "Оценка", "Получение нового опыта"**
  - **Задание 4.1.** Каждому студенту (или малой группе, по усмотрению преподавателя) предоставляется для разбора конкретная ситуация (фабула дела). *Полный перечень ситуаций для разбора представлен в оценочных средствах по дисциплине.*
  - **Пример ситуации для разбора:** «Цифровая травля: дело Марии Волковой» *В одном из престижных вузов города N произошла ситуация, которая привлекла внимание правоохранительных органов и поставила вопросы о границах применения уголовного законодательства в цифровой среде. Мария Волкова, 19-летняя студентка третьего курса факультета журналистики, стала жертвой масштабной кампании киберпреследования. Конфликт начался после того, как девушка опубликовала в социальной сети критическую статью о деятельности студенческого совета университета, обвинив его руководство в нецелевом использовании средств. Председатель студенческого совета Дмитрий Кузнецов, 21 год, не остался в долгу. Используя свои административные возможности и связи, он организовал против Марии целенаправленную кампанию в интернете. Кузнецов создал в мессенджере Telegram закрытый канал «Правда о Волковой», где начал публиковать компрометирующие материалы о девушке. Для усиления воздействия Кузнецов прибег к современным технологиям. Используя приложение FaceSwap с технологией deepfake, он создал порнографические видеоролики, где лицо Марии было наложено на тела порноактрис. Эти материалы были размещены на нескольких порносайтах под настоящим именем девушки с указанием ее учебного заведения и контактных данных. Параллельно Кузнецов запустил в социальных сетях ВКонтакте и Instagram массированную кампанию диффамации. Он создал несколько фейковых аккаунтов и привлек своих сторонников для распространения ложной информации о том, что Мария якобы занимается проституцией, употребляет наркотики и имеет венерические заболевания. Посты сопровождались личными фотографиями девушки, похищенными из ее аккаунтов. Особую жестокость кампания приобрела, когда Кузнецов получил доступ к личной переписке Марии с психологом университета, где она делилась своими проблемами и переживаниями. Эти интимные сообщения были опубликованы в открытом доступе с язвительными комментариями. Апогеем преследования стало создание поддельного аккаунта от имени*

Марии на сайте знакомств с пометкой «ищу спонсора для интимных встреч». В профиле были указаны настоящий номер телефона и адрес проживания девушки. В результате Мария начала получать десятки звонков и сообщений непристойного характера, а к ее общежитию приходили незнакомые мужчины. Психологическое давление оказалось невыносимым. Мария перестала посещать занятия, впала в депрессию и была госпитализирована в психиатрическое отделение с диагнозом «острая стрессовая реакция». Врачи зафиксировали у девушки суицидальные мысли и назначили длительное медикаментозное лечение. Родители Марии обратились в полицию с заявлением о преступлениях, совершенных в отношении их дочери. В ходе проверки было установлено, что Кузнецов действовал не один – к кампании преследования он привлек еще троих студентов, которые помогали ему в создании фейковых аккаунтов и распространении порочащих материалов. Экспертиза компьютерной техники и мобильных устройств подозреваемых подтвердила их причастность к созданию и распространению компрометирующих материалов. Было установлено, что для создания deepfake-видео использовались специализированные программы и значительные вычислительные ресурсы.

Вопросы для разбора (анализа) конкретной ситуации:

- Имеются ли в описанной ситуации признаки составов преступлений против личности? Проведите правовую квалификацию действий каждого из участников.
- Какие нормы уголовного законодательства применимы к созданию и распространению deepfake-контента с изображением другого лица?
- Как должна решаться конкуренция между статьями УК РФ о клевете, оскорблении и нарушении неприкосновенности частной жизни в данной ситуации?
- Какие особенности доказывания преступлений, совершенных в цифровой среде, необходимо учитывать при расследовании данного дела?
- Как оценить степень общественной опасности действий подозреваемых и размер причиненного вреда?
- Какие меры ответственности могут быть применены к лицам, способствовавшим распространению порочащей информации, не являясь ее авторами?
- Проанализируйте возможности применения норм о соучастии в преступлении к действиям группы студентов.
- Какие гражданско-правовые способы защиты нарушенных прав доступны потерпевшей?

- Какую роль в данном деле может играть судебная практика по аналогичным составам преступлений?

Задание (выполняется письменно и/или устно):

- Составьте правовое заключение о квалификации действий каждого из участников инцидента с обоснованием применимых статей УК РФ.
- Разработайте план расследования данного преступления с указанием необходимых следственных действий и экспертиз.
- Подготовьте рекомендации для образовательных учреждений по профилактике киберпреступлений против личности в студенческой среде.

Методические рекомендации по выполнению заданий

- **Методы, способы и приемы выполнения:**
  - **Работа с нормативно-правовыми актами:** Внимательно изучайте диспозиции и санкции статей Особенной части УК РФ (Глава 16, ст. 110, 110.1, 110.2, 117, 119, 128.1, 131-135, 137, 138, 150, 151, 151.2 и др.), а также положения Общей части УК РФ (о понятии преступления, вине, соучастии, множественности и т.д.).
  - **Анализ теоретического материала:** Предоставленный теоретический материал содержит ключевые понятия, проблемы и направления развития законодательства. Используйте его как отправную точку для ваших рассуждений.
  - **Изучение судебной практики:** По возможности (и при указании преподавателя) обращайтесь к Постановлениям Пленума Верховного Суда РФ, обзорам судебной практики по делам соответствующей категории. Это поможет понять, как суды толкуют и применяют нормы права.
  - **Метод юридического анализа (квалификации):** При решении задач и разборе ситуаций последовательно анализируйте все элементы состава преступления: объект, объективную сторону (деяние, последствие, причинно-следственная связь, способ, место, время, обстановка), субъект, субъективную сторону (вина, мотив, цель).
  - **Сравнительно-правовой анализ:** При обсуждении зарубежного опыта или различных подходов к решению правовых проблем сравнивайте их, выявляя достоинства и недостатки.
  - **Моделирование и проектирование:** При разработке предложений по изменению законодательства или планов расследования старайтесь представить, как ваши идеи будут работать на практике.
  - **Групповая дискуссия и мозговой штурм:** Активно участвуйте в обсуждениях, высказывайте свои идеи, даже если они кажутся

нестандартными. Коллективное обсуждение часто приводит к более глубокому пониманию проблемы.
    - **Аргументация:** Любое ваше суждение, вывод или предложение должно быть четко аргументировано ссылками на нормы права, теоретические положения, логические доводы.
- **Типовые решения:**
    - **Алгоритм квалификации деяния:**
        1. Установить фактические обстоятельства дела (что произошло?).
        2. Определить непосредственный объект посягательства (какие общественные отношения нарушены?).
        3. Проанализировать объективную сторону (какие действия/бездействие совершены? каковы последствия? есть ли причинная связь? использовались ли ИТ как способ или орудие?).
        4. Определить субъекта преступления (возраст, вменяемость, специальный субъект, если есть).
        5. Проанализировать субъективную сторону (форма вины – умысел/неосторожность, мотив, цель).
        6. Сделать вывод о наличии/отсутствии состава конкретного преступления. При наличии нескольких составов – решить вопрос о совокупности или конкуренции норм.
- **Инструкции:**
    - При работе с текстом УК РФ обращайте внимание на все слова и формулировки, так как они имеют юридическое значение.
    - При анализе фабул задач выделяйте юридически значимые факты и отбрасывайте второстепенные.
    - Формулируйте свои ответы четко, лаконично, юридически грамотно.
    - Не бойтесь задавать вопросы преподавателю, если что-то непонятно.

Примеры выполнения заданий

- **Пример для Задания 1.1 (Понимание):**
    - *Вопрос:* Объясните своими словами ключевые различия между склонением к самоубийству (ст. 110.1 УК РФ) и доведением до самоубийства (ст. 110 УК РФ).
    - *Примерный ответ студента:* "Основное различие в способах воздействия и направленности умысла. При доведении до самоубийства по ст. 110 УК РФ виновный использует угрозы, жестокое обращение или систематическое унижение достоинства, и эти действия приводят потерпевшего к решению о самоубийстве. То есть, суицид – это результат невыносимых условий, созданных виновным. При склонении по ст. 110.1 УК РФ

виновный целенаправленно возбуждает у потерпевшего желание совершить самоубийство уговорами, предложениями, подкупом или обманом. Здесь нет такого элемента принуждения, как в ст. 110, а есть формирование решимости уйти из жизни. Содействие же (тоже ст. 110.1) – это уже помощь в реализации этого решения: советы, предоставление средств и т.д."

- **Пример для Задания 2.2 (Применение):**
  - *Фрагмент анализа ситуации с гражданкой С. и Л.:* "Действия Л. по распространению ложной информации о том, что С. якобы оказывает интимные услуги за деньги, могут содержать признаки преступления, предусмотренного ч. 2 ст. 128.1 УК РФ (Клевета, совершенная публично с использованием информационно-телекоммуникационных сетей). Распространение личных фотографий С. без ее согласия может квалифицироваться по ст. 137 УК РФ (Нарушение неприкосновенности частной жизни). Угрозы распространить фотографии, если они воспринимались С. реально и имели целью понудить ее к каким-либо действиям, могут рассматриваться в контексте других составов, в зависимости от содержания и цели угроз (например, если это угроза убийством – ст. 119 УК РФ, или если это шантаж с целью получения выгоды – ст. 163 УК РФ). Оскорбительные сообщения сами по себе сейчас декриминализованы в УК, но могут рассматриваться в совокупности с другими действиями как элемент травли. Трудности в доказывании могут быть связаны с идентификацией Л. как владельца фейковых аккаунтов (потребуется IP-адрес, данные от провайдера, экспертиза устройств), а также с доказыванием умысла на распространение именно заведомо ложных сведений для клеветы."
- **Пример для Задания 3.2 (Анализ):**
  - *Фрагмент анализа "виртуального изнасилования":* "В действующем российском уголовном законодательстве понятие "изнасилование" (ст. 131 УК РФ) и "насильственные действия сексуального характера" (ст. 132 УК РФ) традиционно связаны с физическим контактом и применением насилия или угрозой его применения к потерпевшему лицу в реальном мире. Действия, совершаемые исключительно в виртуальной среде с аватарами, даже если они вызывают у пользователя психологические страдания, напрямую под эти составы не подпадают. Отсутствует физическое воздействие на тело потерпевшего. Однако, если такие действия сопровождаются, например, принуждением к созданию и отправке реальных интимных изображений или видео (секстинг под принуждением), то здесь возможна квалификация по ст. 133 УК РФ (Понуждение к действиям сексуального характера).

Проблема "виртуального насилия" требует дальнейшего изучения и, возможно, выработки специальных правовых механизмов, но расширительное толкование существующих статей УК РФ здесь недопустимо из-за принципа nullum crimen sine lege."

3. Проверка практических заданий, выполненных обучающимися

Проверка выполнения практических заданий осуществляется комплексно:

1. **Устный опрос и участие в дискуссиях:** Оценивается активность студента, глубина понимания материала, логика рассуждений, умение аргументировать свою позицию в ходе обсуждения заданий 1.1, 1.3, 2.1, 3.1, 3.2.
2. **Анализ письменных ответов/решений:** Задания 1.2, 2.2, 2.3 (предложения), 3.3 (предложения) могут быть частично или полностью оформлены письменно и сданы на проверку.
3. **Оценка разбора конкретной ситуации (Задание 4.1):** Оценивается письменное правовое заключение, план расследования и рекомендации, а также устная защита и ответы на вопросы по разбору.

Шкала и критерии оценивания (классическая 5-балльная):

- **«Отлично» (5 баллов):**
  - Студент демонстрирует глубокое и всестороннее понимание теоретического материала, безошибочно применяет нормы права к конкретным ситуациям.
  - Ответы полные, аргументированные, логически выстроенные, с использованием корректной юридической терминологии.
  - При решении задач и анализе ситуаций правильно определяет все элементы состава преступления, верно квалифицирует деяния, учитывает судебную практику и доктринальные толкования.
  - Проявляет творческий подход при выполнении заданий на синтез и разработку предложений, его идеи оригинальны и обоснованы.
  - Активно участвует в дискуссиях, его суждения ценны для группы.
  - Письменные работы оформлены грамотно и аккуратно.
  - Показано уверенное владение индикаторами компетенций (для Задания 4.1).
- **«Хорошо» (4 балла):**
  - Студент в целом демонстрирует хорошее понимание материала, правильно применяет нормы права, но допускает отдельные неточности или недостаточно полно раскрывает некоторые аспекты.
  - Ответы в основном аргументированы, но могут содержать незначительные логические пробелы.
  - При квалификации деяний в целом справляется, но может упускать отдельные детали или не всегда полно обосновывать свои выводы.

- Предложения и идеи в целом корректны, но могут не отличаться высокой степенью оригинальности или проработки.
- Участвует в дискуссиях, но не всегда проявляет инициативу.
- Письменные работы содержат незначительные помарки или недочеты в оформлении.
- Показано в основном владение индикаторами компетенций, но с некоторыми недочетами (для Задания 4.1).

- **«Удовлетворительно» (3 балла):**
  - Студент демонстрирует поверхностное понимание основных положений темы, допускает существенные ошибки при применении норм права.
  - Ответы неполные, недостаточно аргументированные, содержат логические ошибки.
  - При квалификации деяний испытывает затруднения, не всегда может правильно определить элементы состава преступления или дать верную квалификацию.
  - Предложения носят формальный характер или недостаточно обоснованы.
  - Пассивен в дискуссиях или его суждения не всегда корректны.
  - Письменные работы содержат ошибки, небрежно оформлены.
  - Индикаторы компетенций освоены на минимально допустимом уровне (для Задания 4.1).
- **«Неудовлетворительно» (2 балла):**
  - Студент демонстрирует непонимание большей части материала, не способен применять нормы права.
  - Ответы отсутствуют, либо являются неверными по существу, неаргументированными.
  - Не справляется с квалификацией деяний.
  - Не способен выполнить задания на анализ и синтез.
  - Не участвует в работе группы или его участие деструктивно.
  - Письменные работы не представлены или выполнены неудовлетворительно.
  - Индикаторы компетенций не освоены (для Задания 4.1).

Задания для самостоятельной работы по данной теме

1. **Изучение судебной практики:** Найдите и проанализируйте 2-3 опубликованных судебных решения (приговора) по ст. 110.1, 128.1 (совершенной с использованием ИТС), 137 УК РФ. Обратите внимание на то, как суд устанавливал факты, какие доказательства использовались, как мотивировалась квалификация. Подготовьте краткий письменный анализ одного из решений.
2. **Подготовка эссе (на выбор):**
   - "Проблемы и перспективы криминализации кибербуллинга в России".

- "Deepfake-технологии как инструмент совершения преступлений против личности: уголовно-правовой аспект".
- "Баланс между свободой выражения мнений в Интернете и защитой личности от диффамации: поиск оптимальной модели".

3. **Сравнительно-правовое исследование:** Изучите законодательство одной или двух зарубежных стран (например, США, Германия, Франция) в части ответственности за кибersталкинг или распространение интимных изображений без согласия ("порноместь"). Подготовьте краткий обзор.
4. **Разработка проекта:** Представьте (в виде тезисов) проект рекомендаций для пользователей социальных сетей по минимизации рисков стать жертвой преступлений против личности в цифровой среде.

Список вопросов для самоконтроля

1. В чем заключается специфика совершения преступлений против личности с использованием информационных технологий?
2. Какие составы преступлений УК РФ наиболее часто применяются при квалификации деяний, связанных с "группами смерти"? В чем их отличие от ст. 110 УК РФ?
3. Дайте определение кибербуллинга. Какие его формы вы знаете? Почему кибербуллинг часто остается безнаказанным?
4. Каковы особенности квалификации клеветы, распространенной в сети Интернет? Какие проблемы возникают при доказывании?
5. Что такое "груминг"? Какие действия могут подпадать под это понятие и как они могут быть квалифицированы по УК РФ?
6. В чем заключается общественная опасность "порномести" и "доксинга"? Какими статьями УК РФ могут охватываться эти деяния?
7. Каковы основные проблемы правового регулирования ответственности за утечки персональных данных и нарушение тайны переписки в ИТС?
8. Какие сложности возникают при расследовании преступлений против личности, совершенных в цифровой среде?
9. Какие превентивные меры, на ваш взгляд, могут быть эффективны для снижения уровня киберпреступности против личности?
10. Каковы, по вашему мнению, перспективы развития уголовного законодательства в сфере противодействия преступлениям против личности с использованием ИТ?

4. Текущий контроль успеваемости по теме № 4

Текущий контроль успеваемости проводится в форме разбора конкретной ситуации.

Шкала и критерии оценивания приведены в оценочных средствах по дисциплине «Преступления в сфере высоких технологий» для данной ОПОП ВО, которые размещены на официальном сайте университета по ссылке https://swsu.ru/sveden/education/eduop/.

ТЕМА № 5
ПРЕСТУПЛЕНИЯ ПРОТИВ ЗДОРОВЬЯ НАСЕЛЕНИЯ И ОБЩЕСТВЕННОЙ НРАВСТВЕННОСТИ, СОВЕРШАЕМЫЕ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

I. ДИСТАНЦИОННАЯ ЧАСТЬ

Задания, выполняемые до начала первого практического занятия по теме № 5

Внеаудиторная (домашняя) самостоятельная работа обучающихся по освоению основных положений темы № 5: предварительное (до начала первого практического занятия по теме) самостоятельное изучение теоретического учебного контента по новой теме дисциплины, разработанного преподавателем и представленного в цифровом формате на портале do.swsu.ru

1.1 Ознакомьтесь с **инструкцией** о порядке организации самостоятельной работы по изучению данной темы и следуйте ей.

1.2. Прочитайте **перечень основных теоретических вопросов**, которые необходимо самостоятельно освоить, и **текст с изложением указанных вопросов**.

1.3 Работая с текстом, вносите по мере чтения необходимые записи в **опорный конспект**, который поможет вам запомнить главное.

Опорный конспект по теме № 5 «Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий»

1. ЗАПОМИНАЕМ ГЛАВНОЕ

1.1 Впишите пропущенные слова, отражающие суть понятий и явлений:

а) Современный незаконный оборот наркотиков характеризуется практически полным переходом на _____ методы распространения контролируемых веществ с использованием «_____», мессенджеров, электронных средств платежа и _____.

б) Крупнейший сайт-«маркетплейс» по продаже наркотиков «Hydra» использовал для доступа клиентов браузер _____ с луковой маршрутизацией, а оплата осуществлялась в _____. Его ликвидация в апреле 2022 года привела к _____ _____.

в) Типичная схема сбыта наркотиков с использованием ИТ включает:

1. Оплата за наркотические средства через _____ системы (например, Qiwi, Webmoney).
2. Конвертация безналичных платежей в _____.
3. Бесконтактная передача наркотиков через _____ и тайники, местонахождение которых уточняется с использованием _____ и прочих цифровых технологий.

г) Отмывание денежных средств, полученных от наркопреступлений, часто включает следующие этапы: аккумуляция средств в _____, их анонимизация через «_____» (специальные сервисы, совершающие множество транзакций) и последующее обналичивание через _____, зачастую с привлечением _____ лиц.

д) Проблемы квалификации деятельности по созданию и обеспечению работы платформ, подобных «Hydra», связаны с тем, что такие действия прямо не запрещены _____ РФ и сложно установить _____ между действиями соучастников и наступившим преступным результатом.

е) В сфере проституции Интернет и ИТС активно используются для: _____ интимных услуг, _____ (в том числе путем завуалированных предложений работы или обмана) и _____ между участниками нелегального рынка.

ж) «Дипфейк» – это созданные с использованием _____ реалистичные видеоролики или изображения, в которых лицо одного человека заменяется на лицо другого. Это создает проблемы не только в контексте порнографии, но и для совершения _____ и _____.

з) Вебкам представляет собой секс-позирование за плату с использованием средств _____. Уголовно-правовая квалификация такой деятельности затруднена, так как формально не создаются _____ материалы (трансляция идет в прямом эфире) и отсутствует _____ сексуальный контакт.

и) «Треш-стримы» – это публичные видеотрансляции, демонстрирующие различные формы аморального поведения, такие как употребление психоактивных веществ с неадекватным поведением, жестокое обращение с _____, пранки, связанные с _____, _____ или _____ граждан, а также сцены издевательств и насилия над «жертвами».

1.2 Заполните пропуски:

А) Основные роли в современных преступных сообществах, занимающихся онлайн-наркоторговлей: 1. Руководитель: общее руководство, координация через сеть «Интернет» и мессенджеры, разработка _____. 2. Администраторы (диспетчеры) территорий: взаимодействие с руководителями, координация распределения _____ между распространителями. 3. Иные участники: менеджеры по персоналу, _____, кураторы интернет-магазинов и складов, операторы, _____ и _____. *К уголовной ответственности, как правило, привлекаются в основном (кто?)* _____.

Б) Некоторые статистические данные и факты о «дикпиках» из материалов лекции: - Примерно _____% женщин хотя бы раз в жизни получали нежелательный дикпик. - В _____% случаев его получению не предшествовала просьба со стороны женщины. - Лишь _____% опрошенных мужчин признались, что отправляли дикпики без согласия женщин. - Ответственность за нежелательную отправку дикпиков законодательно закреплена, например, во _____ (как эксгибиционизм), в штате _____ (США) (штраф), в _____ (тюремное заключение или штраф), в _____ (тюремное заключение или штраф).

1.3 Укажите стрелочкой одно наиболее точное определение или характеристику для каждого понятия (выберите один вариант из предложенных):

А) **Бесконтактный способ передачи наркотиков:**

Передача наркотиков лично из рук в руки в укромном месте.

Отправка наркотиков почтовым отправлением с указанием ложных данных.

Оставление наркотиков в «закладках» или тайниках, координаты которых передаются покупателю цифровым способом.

Продажа наркотиков через легальные аптечные сети по поддельным рецептам.

Б) **«Маркетплейсы» интим-услуг в интернете:**

Сайты, действующие исключительно в «даркнете» для обеспечения анонимности.

Платформы с функционалом интернет-магазинов (поиск, цены, фото, отзывы) для предложения коммерческих сексуальных услуг, часто действующие из стран с легализованной проституцией.

Закрытые форумы для обмена опытом между работниками секс-индустрии

Государственные порталы для регистрации лиц, оказывающих интимные услуги.

В) **Роботизация секс-индустрии (правовой аспект):**

Полностью легальная и детально урегулированная законом сфера деятельности.

Деятельность, сопряженная исключительно с производством медицинских протезов.

Сфера, находящаяся в «серой зоне», порождающая вопросы налогообложения, морали, защиты прав потребителей и возможной уголовной ответственности (например, за услуги, не отвечающие требованиям безопасности).

Запрещенная на международном уровне деятельность.

Г) **«Порноместь»:**

Публикация порнографических материалов с целью получения коммерческой выгоды.

Распространение интимных фото или видео человека без его согласия с целью унизить, шантажировать или отомстить.

Создание пародийных роликов на известные порнографические фильмы.

Просмотр порнографии на рабочем месте.

1.4 Расположите в правильной последовательности предполагаемые этапы отмывания денежных средств, полученных от незаконного оборота наркотиков с использованием ИТ, как они описаны в лекции:

1. Конвертация криптовалюты в безналичные рубли.
2. Пропускание криптовалюты через «миксеры» для анонимизации.
3. Аккумуляция денежных средств (первоначальных доходов) в криптовалюте.
4. Обналичивание денежных средств через банкоматы, часто с использованием подставных лиц («дропов»).

Запишите правильную последовательность цифр: _____

1.5 Установите соответствие между преступным деянием/явлением, совершаемым с использованием ИТ, и его краткой характеристикой:

Преступное деяние/Явление	**Краткая характеристика**
1. Создание «фишингового» сайта интим-услуг	А. Демонстрация в прямом эфире сцен издевательства над человеком за денежное вознаграждение от зрителей.
2. «Треш-стрим» с насилием	Б. Использование генеративных нейросетей для создания видео, где лицо известной личности наложено на тело порноактера, без ее согласия.
3. Рекрутинг в проституцию через соцсети	В. Мошенничество, при котором под видом предложения интим-услуг с жертвы получают предоплату, после чего связь прерывается.
4. Распространение «дипфейк» порнографии	Г. Вовлечение лиц в занятие проституцией путем размещения завуалированных предложений высокооплачиваемой работы (например, в массажных салонах за рубежом).

Заполните таблицу, вписав соответствующие буквы напротив цифр: 1 - ____ 2 - ____ 3 - ____ 4 - ____

1.6 Запишите не менее пяти ключевых проблем правового регулирования и квалификации преступлений против здоровья населения и общественной нравственности, совершаемых с использованием ИТ, упомянутых в лекции:

1. _____
2. _____
3. _____
4. _____
5. _____

2. АНАЛИЗИРУЕМ И СИСТЕМАТИЗИРУЕМ

2.1 Опишите кратко (2-3 аргументированных предложения) по одному примеру из лекционного материала, иллюстрирующему специфику использования ИТ в следующих контекстах:

Контекст	**Пример из лекции и его специфика, связанная с ИТ**
1. Организационная структура наркобизнеса в «даркнете»	
2. Изменение рынка коммерческих сексуальных услуг под влиянием ИТ	
3. Проблемы безопасности и этики, связанные с секс-роботами	
4. Сложности квалификации вебкам-деятельности	
5. Причины распространенности и отправки «дикпиков»	

2.2 Выделите три наиболее значимых, на Ваш взгляд, технологии или цифровые платформы, которые способствуют совершению рассматриваемых в лекции преступлений. Обоснуйте свой выбор, указав их роль.

1. Технология/Платформа: _____ Обоснование и роль: _____ _____ ___
2. Технология/Платформа: _____ Обоснование и роль: _____ _____ ___
3. Технология/Платформа: _____ Обоснование и роль: _____ _____ ___

2.3 Сегодня в ходе лекции меня более всего заставил задуматься вопрос (или аспект проблемы) о _____ , потому что _____ _____.

ВЫВОД ЛИЧНО ДЛЯ СЕБЯ: _____

1.4 Посмотрите **видеоролик** по теме № 5 в ходе чтения текста (параллельно с ним).

Обратите внимание на проблемы квалификации действий, связанных с созданием и обеспечением работы платформ, подобных Hydra, а также незаконных операций с криптовалютами, учитывая отсутствие прямого запрета в УК РФ и сложность установления причинно-следственной связи между действиями соучастников и наступившим преступным результатом.

1.5 Перескажите изученный теоретический материал по вопросам, указанным в инструкции, и опорному конспекту. Воспользуйтесь также следующими **вопросами для самоконтроля**:

1. Какие виды преступлений против здоровья населения и общественной нравственности наиболее часто совершаются с использованием информационных технологий?
2. Опишите механизм работы сайта Hydra и роль криптовалют в незаконном обороте наркотиков.
3. Какие проблемы возникают при квалификации действий, связанных с созданием и обеспечением работы платформ, подобных Hydra?
4. Каким образом преступные сообщества, занимающиеся сбытом наркотиков, используют современные информационные технологии?
5. Какие роли существуют в преступных группах, занимающихся сбытом наркотиков через интернет, и кто чаще всего привлекается к ответственности?
6. Какие изменения произошли на рынке проституции с развитием интернета и какие новые риски возникли для работников секс-индустрии?
7. Какие виды мошенничества распространены в сфере интернет-проституции и продажи девственности?
8. Какие правовые и этические проблемы возникают в связи с роботизацией секс-индустрии и появлением секс-роботов?
9. Какова текущая ситуация с уголовной ответственностью за оборот порнографических материалов в России и какие изменения предлагаются?
10. Что такое дипфейки и какие правовые проблемы возникают в связи с их распространением, особенно в контексте порнографии?
11. Опишите суть вебкам-бизнеса и проблемы с его уголовно-правовой квалификацией.
12. Что такое дикпики, почему они получили распространение и какая ответственность предусмотрена за их отправку в разных странах и в России?
13. Что такое треш-стримы и какие виды аморального поведения они демонстрируют? Какие проблемы возникают при привлечении треш-стримеров к ответственности?

14. Каким образом деструктивные организации используют информационные технологии для пропаганды, вербовки и коммуникации?

1.6 Возьмите с собой на практическое занятие свой **опорный конспект** по теме № 5.

1.7 Выполните **входное тестирование** по теме № 5.

Ответьте на вопросы и выполните задания в тестовой форме по теме № 5:

Вопросы в закрытой форме:

1. Укажите, какой из перечисленных интернет-ресурсов являлся одним из крупнейших маркетплейсов по продаже наркотиков в российском сегменте «даркнета» до его ликвидации в 2022 году: а) Silk Road б) AlphaBay в) Hydra г) DarkMarket д) Wall Street Market
2. Какая технология, обеспечивающая анонимность пользователей за счет многоуровневого шифрования и «луковой маршрутизации», активно использовалась покупателями для доступа к площадкам типа Hydra? а) VPN (Virtual Private Network) б) Proxy-сервер в) Tor (The Onion Router) г) I2P (Invisible Internet Project) д) Blockchain
3. Согласно представленному материалу, какая основная проблема квалификации возникает применительно к созданию и обеспечению работы платформ, подобных Hydra, с точки зрения российского уголовного законодательства? а) Отсутствие прямого запрета на создание таких платформ в УК РФ. б) Сложность доказывания умысла организаторов на сбыт наркотиков. в) Невозможность установления личности администраторов из-за использования анонимайзеров. г) Проблема определения юрисдикции, так как серверы часто находятся за рубежом. д) Отсутствие потерпевших, заявивших о причиненном вреде.
4. В какой момент, согласно сложившейся практике, считается оконченным преступление по сбыту наркотических средств, если передача происходит бесконтактным способом через «закладку»? а) В момент получения оплаты от покупателя. б) В момент помещения наркотического средства в тайник («закладку»). в) В момент получения покупателем информации о местонахождении «закладки». г) В момент фактического изъятия наркотического средства покупателем из «закладки». д) В момент фасовки наркотического средства для последующей «закладки».
5. Каким образом, согласно тексту, информационно-телекоммуникационные сети (ИТС) преимущественно используются в современной индустрии порнографии? а) Для организации закрытых показов в кинотеатрах. б) Для распространения физических носителей (DVD, Blu-Ray). в) Как основной и практически единственный канал распространения продукции. г) Исключительно для рекламы студий,

снимающих порнографические фильмы. д) Для координации актеров и съемочных групп.

6. Какая статья Уголовного кодекса РФ формально устанавливает ответственность за незаконные изготовление и оборот порнографических материалов или предметов? а) ст. 135 УК РФ б) ст. 240 УК РФ в) ст. 241 УК РФ г) ст. 242 УК РФ д) ст. 242.1 УК РФ
7. Что является одной из ключевых проблем при квалификации деятельности вебкам-моделей по статье 242 УК РФ (Незаконные изготовление и оборот порнографических материалов)? а) Отсутствие предварительной записи и передачи видеофайла, так как работа ведется в режиме прямой трансляции. б) Несовершеннолетие большинства моделей. в) Использование зарубежных платформ для трансляций. г) Добровольное согласие моделей на участие в трансляциях. д) Невозможность точной идентификации зрителей.
8. Какая технологическая функция мобильных устройств, по мнению автора материала, способствовала массовому распространению «дикпиков» в начале 2010-х годов? а) Bluetooth б) NFC (Near Field Communication) в) Wi-Fi Direct г) AirDrop д) MMS (Multimedia Messaging Service)
9. Деятельность каких организаций, сопряженная с насилием над гражданами или побуждением к отказу от исполнения гражданских обязанностей и использующих ИТС для своей пропаганды, подпадает под действие статьи 239 УК РФ? а) Коммерческие организации с иностранным участием. б) Политические партии экстремистской направленности. в) Деструктивные религиозные или общественные объединения и некоммерческие организации. г) Финансовые пирамиды, использующие интернет-рекламу. д) Группы футбольных фанатов, организующие беспорядки.
10. Какая основная сложность, согласно тексту, возникает при привлечении к уголовной ответственности организаторов «треш-стримов»? а) Большинство действий участников содержат лишь составы административных правонарушений или являются ненаказуемыми. б) Трудность идентификации зрителей, заказывающих противоправные действия. в) Использование иностранных стриминговых платформ. г) Добровольное участие «жертв» в трансляциях. д) Отсутствие четкого определения «треш-стрима» в законодательстве.

Вопросы в открытой форме:

11. Специальные сервисы, используемые в схемах отмывания денег от наркоторговли для анонимизации криптовалютных транзакций путем совершения множества трудноотслеживаемых операций, называются _____.
12. Сайты, предоставляющие услуги по поиску, сравнению цен, просмотру фотографий и отзывов в сфере коммерческих сексуальных услуг,

функционирующие по аналогии с интернет-магазинами, в тексте обозначаются как _____ интим-услуг.

13. Технология, основанная на использовании генеративных нейросетей для создания реалистичных видеороликов, в которых лицо одного человека заменяется на лицо другого, что может использоваться для создания порнографии, мошенничества или дискредитации, называется _____.
14. Прямая видеотрансляция сексуального позирования или выполнения различных действий сексуального характера по просьбе платных подписчиков с использованием средств видеоконференцсвязи – это _____.
15. Фотография мужского полового органа, отправляемая, как правило, без согласия адресата, через мобильные устройства или личные сообщения в социальных сетях, получила устойчивое наименование _____.

Вопросы на установление правильной последовательности:

16. Расположите в правильной хронологической последовательности этапы типичной схемы сбыта наркотиков с использованием информационных технологий, описанной в тексте:
    1. Передача покупателю информации о местонахождении «закладки» с использованием GPS или иных цифровых технологий.
    2. Конвертация безналичных платежей в криптовалюту.
    3. Получение оплаты за наркотические средства через электронные платежные системы.
    4. Бесконтактная передача наркотиков покупателю через «закладку» или тайник.
17. Установите последовательность действий при отмывании денежных средств, полученных от незаконного оборота наркотиков, согласно описанной в тексте схеме:
    1. Пропускание криптовалюты через «миксеры» для анонимизации.
    2. Аккумулирование денежных средств в криптовалюте.
    3. Обналичивание через банкоматы, часто с привлечением подставных лиц.
    4. Конвертация криптовалюты в безналичные рубли.
18. Восстановите последовательность этапов вовлечения женщин в занятие проституцией посредством сети Интернет, как это следует из материала:
    1. Предложение высокооплачиваемой работы (иногда с обманом относительно характера деятельности).
    2. Размещение завуалированных предложений о работе в социальных сетях или на сайтах.
    3. Фактическое вовлечение в занятие проституцией, иногда сопряженное с торговлей людьми.

4. Установление контакта с потенциальной жертвой.

19. Расположите в логической последовательности этапы взаимодействия в рамках организованного «вебкам-бизнеса», описанного в тексте, с точки зрения модели:
    1. Привлечение клиентов через красивые фото или живые трансляции в социальных сетях.
    2. Выполнение различных просьб клиента, в том числе сексуального характера, в режиме прямой трансляции.
    3. Приглашение потенциального клиента в закрытый чат.
    4. Достижение договоренности об оплате и времени сеанса.
20. Установите последовательность действий мошенников при совершении преступления под видом оказания интим-услуг через интернет (схема с предоплатой):
    1. Предложение потенциальным клиентам внести «предоплату» для подтверждения «серьезности намерений».
    2. Размещение объявлений и анкет с выгодными условиями интимного контакта.
    3. Обрыв связи или запрос дополнительных сумм денег после получения предоплаты.
    4. Установление контакта с потенциальным клиентом.

Вопросы на установление соответствия:

21. Установите соответствие между ролью участника преступного сообщества, занимающегося сбытом наркотиков, и его основной функцией: А) Руководитель Б) Администратор (диспетчер) территории В) Курьер (закладчик) Г) Менеджер по персоналу
    1. Непосредственное размещение наркотических средств в тайниках.
    2. Общее руководство деятельностью группы, разработка планов.
    3. Подбор и вербовка новых участников преступной группы.
    4. Координация распределения наркотических средств между непосредственными распространителями на определенной территории.
22. Установите соответствие между статьей Уголовного кодекса РФ и составом преступления, имеющим отношение к сексуальной эксплуатации или преступлениям против половой свободы и неприкосновенности, упомянутым в контексте интернет-преступности: А) ст. 240 УК РФ Б) ст. 241 УК РФ В) ст. 134 УК РФ Г) ст. 127.1 УК РФ
    1. Половое сношение и иные действия сексуального характера с лицом, не достигшим шестнадцатилетнего возраста.
    2. Организация занятия проституцией.
    3. Вовлечение в занятие проституцией.
    4. Торговля людьми.
23. Установите соответствие между правовой проблемой, связанной с использованием секс-роботов, и ее сущностью: А) Проблема

безопасности робота Б) Проблема конфиденциальности данных В) Этическая проблема создания роботов-детей/животных Г) Проблема легальности деятельности «досуговых центров»

1. Накопление и возможное неправомерное использование информации об интимных привычках хозяина.
2. Отсутствие четкого правового регулирования и налогообложения.
3. Возможность причинения вреда человеку действиями робота или используемыми материалами.
4. Отсутствие технических и правовых препятствий для создания роботов, имитирующих уязвимые категории.

24. Установите соответствие между видом аморального поведения, демонстрируемого в «треш-стримах», и его конкретным проявлением: А) Употребление психоактивных веществ Б) Жестокое обращение с животными В) Пранки Г) Сцены издевательства
    1. Организация розыгрышей, связанных с оскорблением или унижением их участников.
    2. Публичная демонстрация побоев или унижения «жертвы» стрима.
    3. Трансляция немедицинского употребления наркотиков, сопровождающегося неадекватным поведением.
    4. Демонстрация действий, причиняющих страдания или гибель животным (даже если не всегда достигает состава ст. 245 УК РФ).
25. Установите соответствие между страной и особенностями ее законодательства в отношении нежелательной отправки «дикпиков», как это описано в тексте: А) Франция Б) Техас (США) В) Нидерланды Г) Германия
    1. Предусмотрен штраф в размере 500 долларов.
    2. Рассматривается как несанкционированное распространение порнографических материалов (§ 184 УК), наказуемо тюремным заключением до одного года или штрафом.
    3. Может рассматриваться как акт эксгибиционизма (до 1 года тюрьмы и штраф 15 000 евро) или отправка сообщения, противоречащего приличиям (штраф 750 евро).
    4. Является преступлением (ст. 240 УК), наказуемым заключением на срок до 2 месяцев или штрафом до 9000 евро.

II. АУДИТОРНАЯ ЧАСТЬ

Практическое занятие № 5
«Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий»

Цель практического занятия – приобретение обучающимися практического опыта в применении знаний, полученных при самостоятельном освоении темы № 5, в производственных ситуациях.

Планируемые результаты обучения:

Знать:	**Уметь:**	**Иметь опыт деятельности:**
содержание норм, устанавливающих ответственность за преступные деяния, связанные с преступлениями в сфере высоких технологий, особенности их реализации; методологические основы реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; содержание постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, связанных с уголовно-правовым регулированием ответственности за преступления в сфере высоких технологий;	использовать информацию о нормах, устанавливающих ответственность за преступления в сфере высоких технологий, в целях их реализации; применять нормы особенной части уголовного права, регулирующие ответственность за преступления в сфере высоких технологий; применять нормы особенной части уголовного права, регулирующие ответственность за преступления в сфере высоких технологий с учётом постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований; давать полную и точную квалификацию преступлений в сфере высоких технологий, с учётом положений	по обобщению и анализу информации, имеющей значение для реализации правовых норм в сфере установления ответственности за преступления в сфере высоких технологий; по реализации решений, связанных с применением норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий; по обобщению и анализу постановлений Пленума Верховного Суда РФ, учебной литературы и научных источников, иных актов судебной практики, официальных и доктринальных толкований, касающихся норм особенной части уголовного права, регулирующих ответственность за преступления в сфере высоких технологий;

особенности оценки на соответствие признакам преступления (квалификации) конкретных преступлений в сфере высоких технологий, предусмотренных уголовным законодательством; способы толкования норм уголовного законодательства, позволяющие вычленить из их текста основные юридически значимые признаки преступных деяний, связанных с высокими технологиями, и сопоставить их с признаками преступления; особенности толкования норм уголовного законодательства, устанавливающих ответственность за конкретные преступления в сфере высоких технологий, позволяющие разграничить между собой смежные составы преступлений при наличии конкуренции норм	Общей и Особенной части уголовного законодательства, разъяснений Пленума Верховного Суда РФ; толковать положения актов уголовного законодательства, касающиеся высоких технологий, основываясь на общих принципах толкования нормативных актов; разъяснять содержание норм уголовного законодательства, предусматривающих ответственность за совершение конкретных преступлений в сфере высоких технологий, с учётом судебной практики и доктрины уголовного права; устанавливать содержание оценочных признаков норм уголовного законодательства, регулирующих ответственность за преступления в сфере высоких технологий, а также признаков, позволяющих разграничить между собой смежные преступные деяния при наличии конкуренции норм	по принятию решений, связанных с оценкой на соответствие конкретных деяний, связанных с высокими технологиями, признакам преступления; по применению основных подходов к толкованию норм уголовного законодательства Российской Федерации, касающихся высоких технологий, и вычленению признаков конкретного деяния; по выявлению точного содержания норм уголовного законодательства, устанавливающих общие условия уголовной ответственности и освобождения от неё, а также признаки конкретных составов преступлений, связанных с преступлениями в сфере высоких технологий; по применению приёмов научного мышления, позволяющих устанавливать смысл нормоустановлений уголовно-правового характера, касающихся высоких технологий, в условиях правовой

неопределённости, коллизий правового регулирования, конкуренции норм

Необходимое материально–техническое оборудование: ноутбук и (или) мобильные устройства преподавателя и обучающихся.

ПЛАН ПРАКТИЧЕСКОГО ЗАНЯТИЯ № 5

1. Уточнение и (или) углубление отдельных вопросов по теме № 5.
2. Выполнение обучающимися практических заданий.
3. Проверка практических заданий, выполненных обучающимися.
4. Текущий контроль успеваемости по теме № 5

1. Уточнение и (или) углубление отдельных вопросов по теме № 5

Консультация преподавателя

Студенты методом мозгового штурма формируют перечень вопросов, которые при самостоятельном освоении темы дома или при тестировании остались для них непонятными или показались сложными и (или) спорными. Преподаватель по результатам тестирования при необходимости добавляет в сформированный обучающимися список вопросы, которые, с его точки зрения, требуется уточнить или углубить.

Определяя с помощью поднятых рук количество студентов, считающих сложным конкретный вопрос из сформированного списка, преподаватель устанавливает вопросы, по которым сразу же проводит групповую консультацию.

Если в пояснениях нуждаются 1-2 человека, преподаватель индивидуально консультирует их в ходе практического занятия.

2. Выполнение обучающимися практических заданий

На данном практическом занятии выполнение обучающимися практических заданий проводится по технологии проблемно-ориентированного обучения с элементами кейс-стади и проектной деятельности.

ПЕРЕЧЕНЬ ВЫПОЛНЯЕМЫХ ЗАДАНИЙ

Аудиторное занятие 1: Бесконтактное распространение наркотических средств и психотропных веществ

1. **Уровень "Понимание" (20 минут):**
    - Задание 1.1: На основе предоставленного теоретического материала и собственных изысканий, объясните своими словами механизм функционирования типичного онлайн-магазина по продаже наркотиков (по аналогии с "Hydra"). Составьте схему,

отражающую ключевые роли участников (организатор, администратор, оператор, курьер, закладчик, покупатель, специалист по отмыванию денег) и их взаимодействие с использованием ИТ. Обсудите в малых группах (3-4 человека) основные технологические элементы, обеспечивающие анонимность и безопасность для преступников.

2. **Уровень "Применение" (30 минут):**
    - Задание 1.2 (Кейс-стади): Гражданин П., действуя по указанию неустановленного лица через мессенджер "Telegram", получил информацию о местонахождении крупной партии мефедрона. Он расфасовал наркотическое средство на мелкие дозы и, используя координаты GPS, полученные от "куратора", разместил 20 "закладок" в различных районах города. Информацию о местоположении "закладок" с фотографиями он передал "куратору" через тот же мессенджер. Оплату за свои действия П. получал на электронный кошелек, после чего конвертировал средства в криптовалюту.
        - Дайте уголовно-правовую квалификацию действиям гражданина П. Аргументируйте свой ответ, ссылаясь на нормы УК РФ и Постановления Пленума ВС РФ.
        - Какие проблемы могут возникнуть при доказывании использования П. именно информационно-телекоммуникационных сетей для сбыта, а не просто средств мобильной связи для личного общения?
3. **Уровень "Анализ" (30 минут):**
    - Задание 1.3: Проанализируйте и сравните традиционные (контактные) и современные (бесконтактные, с использованием ИТ) способы распространения наркотиков. Выделите не менее 3 преимуществ и 3 недостатков каждого способа с точки зрения: а) организаторов наркобизнеса; б) правоохранительных органов. Обсудите, почему признак "с использованием ... электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет")" не всегда автоматически применим при сбыте через закладки.

Аудиторное занятие 2: Проституция и торговля людьми с использованием ИТ

1. **Уровень "Понимание" (20 минут):**
    - Задание 2.1: Используя теоретический материал, объясните, каким образом информационные технологии трансформировали рынок коммерческих сексуальных услуг. Опишите функционал типичного "маркетплейса" интим-услуг. Обсудите в группах, как ИТ повлияли на роль сутенеров и риски для лиц, вовлеченных в проституцию.

2. **Уровень "Применение" (30 минут):**
    - Задание 2.2 (Кейс-стади): Гражданка Иванова создала закрытую группу в социальной сети "ВКонтакте", где размещала анкеты девушек, предлагающих интимные услуги, с указанием цен и условий. Клиенты связывались с Ивановой через личные сообщения, она организовывала встречи и получала 20% от гонорара девушек. Девушки были совершеннолетними и формально действовали добровольно, но Иванова контролировала их график и угрожала публикацией компрометирующих сведений в случае отказа от "клиентов".
        - Квалифицируйте действия Ивановой. Какие статьи УК РФ могут быть применимы? Обоснуйте.
        - Изменится ли квалификация, если будет установлено, что одна из девушек была несовершеннолетней, но скрывала свой возраст, а Иванова не предприняла достаточных мер для его проверки?
3. **Уровень "Анализ" (30 минут):**
    - Задание 2.3: Проанализируйте феномен "продажи девственности" через интернет-агентства. Какие составы преступлений, предусмотренные УК РФ, могут охватывать деятельность таких агентств и их "скаутов"? Аргументируйте возможность (или невозможность) квалификации таких действий как торговля людьми (ст. 127.1 УК РФ). Какие этические и правовые проблемы порождает роботизация секс-индустрии (на примере "отелей с секс-куклами")?

Аудиторное занятие 3: Порнография и ее распространение в сети Интернет

1. **Уровень "Понимание" (15 минут):**
    - Задание 3.1: Объясните, почему квалифицирующий признак использования ИТС в ст. 242 УК РФ (Незаконные изготовление и оборот порнографических материалов или предметов) можно считать избыточным в современных условиях. Какова, на ваш взгляд, текущая тенденция правоприменения по данной статье (исходя из теоретического материала и общих знаний)?
2. **Уровень "Применение" (25 минут):**
    - Задание 3.2 (Кейс-стади): Гражданин С. с помощью специализированного ПО создал несколько видеороликов ("дипфейков"), где лицо его бывшей коллеги, гражданки Н., было наложено на тела актрис в порнографических сценах. Эти ролики С. анонимно разместил на нескольких файлообменниках и тематических форумах, а ссылки отправил общим знакомым С. и Н.

        - Дайте уголовно-правовую оценку действиям С. По каким статьям УК РФ он может быть привлечен к ответственности? Обоснуйте свой ответ.
        - Какие сложности могут возникнуть при доказывании вины С. и определении порнографического характера созданных материалов?
3. **Уровень "Анализ" (25 минут):**
    - Задание 3.3: Проведите анализ аргументов "за" и "против" декриминализации оборота "обычной" порнографии (не связанной с несовершеннолетними, насилием и т.п.) в России. Какие виды порнографического контента, на ваш взгляд, должны оставаться под безусловным запретом и почему?
4. **Уровень "Синтез" (15 минут):**
    - Задание 3.4: В малых группах разработайте и предложите не менее двух законодательных инициатив (конкретных формулировок или идей для дополнения УК РФ/КоАП РФ), направленных на борьбу с распространением "дипфейков" порнографического характера и "порноместью".

Аудиторное занятие 4: Веб-кам, дикпики и иные формы сексуализированного онлайн-контента

1. **Уровень "Понимание" (20 минут):**
    - Задание 4.1: Дайте определение понятиям "веб-кам модель", "дикпик". Опишите типичные схемы организации веб-кам бизнеса (индивидуальный и студийный). Объясните, почему получение "дикпика" в большинстве случаев является нежелательным для адресата и какие мотивы могут быть у отправителей.
2. **Уровень "Применение" (25 минут):**
    - Задание 4.2 (Кейс-стади): Гражданка К. регулярно проводила приватные онлайн-трансляции сексуального характера для платных подписчиков на специализированной платформе. Запись трансляций не велась ни ею, ни платформой. Клиенты оплачивали доступ к трансляциям и могли давать "задания" К. в чате.
        - Возможно ли привлечь К. к уголовной ответственности по ст. 242 УК РФ? Аргументируйте. Какие еще статьи УК РФ или КоАП РФ потенциально могут быть применены?
    - Задание 4.3 (Кейс-стади): Гражданин Л. систематически отправлял фотографии своих половых органов (дикпики) незнакомым женщинам в социальных сетях, чьи профили были открыты. На просьбы прекратить не реагировал.
        - Дайте правовую оценку действиям Л. по действующему российскому законодательству. Существуют ли эффективные правовые механизмы для защиты от такого поведения?

3. **Уровень "Анализ" (35 минут):**
    - Задание 4.4: Сравните подходы к правовой оценке и ответственности за отправку нежелательных интимных фотографий ("дикпиков") в России и 2-3 зарубежных странах (на основе теоретического материала и дополнительного поиска). Выявите сильные и слабые стороны российского подхода. Обсудите, почему деятельность веб-кам моделей часто находится в "серой зоне" законодательства и какие правовые проблемы это порождает.

Аудиторное занятие 5: Треш-стримы и деятельность деструктивных организаций в ИТ-пространстве

1. **Уровень "Понимание" (20 минут):**
    - Задание 5.1: Объясните феномен "треш-стримов". Приведите не менее 3 примеров контента, характерного для треш-стримов. Каким образом деструктивные организации (в контексте ст. 239 УК РФ) используют информационные технологии для своей деятельности?
2. **Уровень "Применение" (25 минут):**
    - Задание 5.2 (Кейс-стади): Блогер М. во время прямой трансляции на видеохостинге, получая денежные пожертвования (донаты) от зрителей, выполнял их "задания": в частности, унижал свою сожительницу, нанес ей несколько ударов по лицу (не повлекших вреда здоровью, по заключению СМЭ), заставил выпить большое количество алкоголя, после чего она потеряла сознание. Трансляцию смотрели несколько тысяч человек.
        - Квалифицируйте действия М. Какие сложности возникнут при применении существующих норм УК РФ?
3. **Уровень "Анализ" (20 минут):**
    - Задание 5.3: Проанализируйте, почему многие действия, совершаемые в ходе "треш-стримов", остаются вне поля зрения уголовного закона или влекут лишь административную ответственность. Какие пробелы в законодательстве способствуют этому?
4. **Уровень "Синтез" (15 минут):**
    - Задание 5.4: В малых группах разработайте предложения по дополнению УК РФ (например, ст. 115, 116, 213, 245) или введению новых составов, направленных на эффективное противодействие "треш-стримам" и публичной демонстрации насилия и унижения с использованием ИТС. Обоснуйте необходимость предложенных изменений.

Аудиторное занятие 6: Текущий контроль в форме подготовки мини-проекта по теме "Преступления против здоровья населения и

общественной нравственности, совершаемые с применением информационных технологий"

- **Уровень "Оценка", "Получение нового опыта" (80 минут на аудиторную работу + самостоятельная доработка):** Студенты делятся на малые группы (3-4 человека). Каждая группа выбирает одну из предложенных тем для мини-проекта. В течение аудиторного занятия группы разрабатывают структуру проекта, определяют задачи, методы исследования, собирают и анализируют первичную информацию, готовят тезисы и основные положения.
    - **Задачи мини-проекта (общие для всех тем, конкретизируются в зависимости от выбранной темы):**
        - Использовать и проанализировать информацию о нормах, устанавливающих ответственность за соответствующие преступления, и особенностях их реализации
        - Продемонстрировать умение применять нормы Особенной части УК РФ к смоделированным или реальным ситуациям
        - Применить нормы Особенной части УК РФ с учётом судебной практики, доктринальных толкований
        - Оценить конкретные деяния (реальные или гипотетические) на предмет соответствия признакам преступления
        - Осуществить вычленение признаков деяния и сопоставить их с признаками состава преступления, используя методы толкования
        - Предложить решение вопроса о выборе нормы при возможной конкуренции, разграничить смежные составы
        - Разработать предложения по совершенствованию законодательства или правоприменительной практики.
    - **Формат представления результатов:** Краткая презентация основных идей и предложений на занятии (5-7 минут на группу). Окончательное оформление мини-проектов (в виде аналитической записки/эссе объемом 7-10 страниц) осуществляется студентами после занятия в рамках самостоятельной работы. Выполненный проект направляется преподавателю в электронном виде в установленный срок. Контроль выполнения осуществляется дистанционно.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ЗАДАНИЙ

- **Общие принципы:**
    - **Активная работа с источниками:** Используйте текст Уголовного кодекса РФ (в актуальной редакции), Постановления Пленума Верховного Суда РФ по соответствующим категориям дел, научные статьи, учебную литературу. Приветствуется поиск

и анализ актуальной судебной практики (например, через системы "КонсультантПлюс", "Гарант" или сайт СудебныеРешения.рф).
    - **Критическое мышление:** Не принимайте на веру все утверждения. Анализируйте, сопоставляйте, формулируйте собственную позицию.
    - **Командная работа и дискуссия:** Обсуждайте задания в малых группах. Умение аргументировать свою точку зрения и слышать оппонента – важный навык юриста.
    - **Творческий подход:** Для заданий на "синтез" и "получение нового опыта" не бойтесь предлагать нестандартные решения, но всегда обосновывайте их.
- **Методы, способы и приемы выполнения заданий по уровням:**
    - **Понимание:** Используйте методы перефразирования, составления логических схем, интеллект-карт (mind maps) для структурирования информации. Объясняйте сложные термины простыми словами.
    - **Применение (решение кейсов):**
        1. Внимательно изучите фабулу дела.
        2. Определите объект посягательства.
        3. Проанализируйте объективную сторону (деяние, последствие, причинно-следственная связь, способ, место, время, обстановка). Особое внимание уделите роли ИТ.
        4. Определите субъекта преступления.
        5. Установите субъективную сторону (форма вины, мотив, цель).
        6. Сделайте вывод о наличии/отсутствии состава преступления и квалифицируйте деяние по соответствующей статье (части, пункту) УК РФ.
        7. Обоснуйте каждый элемент вывода ссылками на закон и материалы дела.
    - **Анализ:** Применяйте методы сравнения (выявление общего и различного), классификации, выявления причинно-следственных связей, анализа сильных и слабых сторон (SWOT-анализ для проблемных ситуаций). Разлагайте сложные явления на составные части.
    - **Синтез:** Используйте метод "мозгового штурма" для генерации идей. При разработке предложений по изменению законодательства, старайтесь формулировать их юридически корректно, по аналогии с существующими нормами. Соединяйте разрозненные элементы в новую, целостную систему.
    - **Оценка (в рамках мини-проекта):** Определяйте ценность, эффективность, значимость тех или иных правовых явлений, норм, предложений. Используйте четкие критерии для оценки.

    - **Получение нового опыта (в рамках мини-проекта):** Проводите небольшие исследования, проектируйте модели правового регулирования, разрабатывайте практические рекомендации.
- **Типовые решения (пример для задачи на квалификацию):**
    - *Фабула:* Гражданин А. через Интернет продал гражданину Б. наркотическое средство.
    - *Решение (схема):*
        1. *Объект:* Общественные отношения в сфере охраны здоровья населения и установленного порядка оборота наркотических средств.
        2. *Объективная сторона:* Незаконный сбыт наркотических средств (передача от А. к Б.), совершенный с использованием информационно-телекоммуникационных сетей (Интернет). Действия А. окончены с момента выполнения им всех необходимых действий по передаче наркотика Б. (например, сообщение места закладки после оплаты).
        3. *Субъект:* Вменяемое физическое лицо, достигшее 16-летнего возраста (гражданин А.).
        4. *Субъективная сторона:* Прямой умысел (А. осознавал, что сбывает наркотик, и желал этого).
        5. *Квалификация:* Действия А. следует квалифицировать по соответствующей части ст. 228.1 УК РФ с учетом п. "б" ч. 2 (использование ИТС).

ПРИМЕРЫ ВЫПОЛНЕНИЯ ЗАДАНИЙ

- **Пример задания на "Понимание" (по Занятию 1):**
    - *Задание:* Объясните роль "закладчика" в схеме бесконтактного сбыта наркотиков.
    - *Пример ответа (кратко):* "Закладчик" – это низшее звено в иерархии онлайн-наркобизнеса. Его функция – получение партии наркотика от куратора (часто тоже через "закладку" или "мастер-клад"), ее возможная дальнейшая расфасовка и размещение мелких доз в тайниках ("закладках") в различных местах. Координаты и фото тайников он передает куратору через анонимные мессенджеры или специальные платформы. Оплату получает на электронные кошельки или в криптовалюте. Он не контактирует напрямую ни с организаторами, ни с покупателями, что обеспечивает определенную безопасность для остальной части сети, но делает его самого наиболее уязвимым для задержания."
- **Пример задания на "Применение" (по Занятию 3, кейс 3.2):**
    - *Задание:* Квалифицируйте действия С. (создание и распространение дипфейк-порно с коллегой).

- *Пример ответа (схема):*
    1. *Деяние 1: Создание дипфейков.* Объективно С. изготовил материалы порнографического характера (если экспертиза подтвердит). Субъективно – прямой умысел, цель – распространение. Возможно, ст. 242 УК РФ (изготовление в целях распространения).
    2. *Деяние 2: Распространение дипфейков.* Объективно С. разместил на файлообменниках и форумах, разослал ссылки. Субъективно – прямой умысел. Возможно, ст. 242 УК РФ (распространение).
    3. *Дополнительно:* Если будет доказан умысел на унижение чести и достоинства Н., выраженный в неприличной форме, и публичность распространения – ст. 137 УК РФ (нарушение неприкосновенности частной жизни, т.к. использовано ее изображение без согласия для создания интимного контента) и/или ст. 128.1 УК РФ (клевета, если сведения ложные и порочащие, а порнографический характер будет доказан).
    4. *Проблема:* Доказывание порнографического характера дипфейка, умысла, цели.
    5. *Вывод:* Действия С. могут быть квалифицированы по совокупности преступлений, например, ч.1 ст.242 и ч.1 ст.137 УК РФ. Необходима экспертиза материалов.

- **Пример задания на "Анализ" (по Занятию 2):**
    - *Задание:* Проанализируйте риски для "работниц" в онлайн-проституции.
    - *Пример ответа (тезисно):* "Несмотря на кажущуюся большую автономию и безопасность (отсутствие сутенера "на улице"), онлайн-проституция несет свои риски: 1. **Физическое насилие и обман со стороны клиентов:** встречи все равно происходят оффлайн, риск нападения, неоплаты, кражи сохраняется. 2. **Цифровое насилие:** шантаж публикацией материалов, деанонимизация, кибербуллинг. 3. **Зависимость от платформ:** блокировка аккаунта, непрозрачные правила, комиссии. 4. **Психологические проблемы:** стигматизация, даже если деятельность анонимна. 5. **Отсутствие правовой защиты:** нелегальный статус мешает обращаться в полицию. 6. **Риск вовлечения в торговлю людьми:** онлайн-рекрутинг может быть обманчивым."
- **Пример задания на "Синтез" (по Занятию 4):**
    - *Задание:* Предложите законодательную инициативу по борьбе с "дикпиками".

- *Пример ответа (идея):* "Предлагается дополнить Кодекс Российской Федерации об административных правонарушениях статьей следующего содержания: "Статья Х.Х. Отправка изображения интимного характера без согласия получателя. 1. Отправка изображения обнаженных гениталий или полового акта лицу, не выразившему предварительного согласия на его получение, с использованием электронных или информационно-телекоммуникационных сетей, – влечет наложение административного штрафа на граждан в размере от ... до ... рублей. 2. Те же действия, совершенные повторно в течение года после наложения административного взыскания за аналогичное правонарушение, либо совершенные в отношении заведомо несовершеннолетнего, – влекут наложение административного штрафа... или административный арест на срок до пятнадцати суток". Обоснование: необходимость защиты частной жизни и психологического комфорта граждан от нежелательного сексуализированного контента, массовость явления, недостаточная эффективность существующих норм."

Пример выполнения мини-проекта (схематично, по теме "Проблемы квалификации и доказывания организации и участия в преступном сообществе (преступной организации), специализирующемся на бесконтактном сбыте наркотиков с использованием ИТ")

1. **Введение:**
   - Актуальность: рост онлайн-наркоторговли, высокая латентность, сложность доказывания ст. 210 УК РФ.
   - Цель: выявить проблемы квалификации и доказывания по ст. 210 УК РФ применительно к онлайн-наркосообществам и предложить пути их решения.
   - Задачи: изучить теорию, законодательство (УК, УПК, ФЗ об ОРД), ППВС, судебную практику; проанализировать особенности структуры и функционирования онлайн-наркосообществ; выявить типичные проблемы доказывания; разработать рекомендации.
2. **Основная часть:**
   - **Глава 1. Теоретико-правовые основы ст. 210 УК РФ и специфика ИТ-преступности.**
     - Признаки преступного сообщества (сплоченность, иерархия, цель и т.д.) – как они проявляются в онлайн-среде?
     - Особенности использования ИТ: анонимность, шифрование, криптовалюты, даркнет.
   - **Глава 2. Анализ судебной практики и проблем квалификации.**
     - Подборка 5-7 приговоров по ст. 210 + ст. 228.1 (с ИТС). Анализ доказательственной базы

        - Проблемы:
            - Доказывание устойчивости и сплоченности виртуальной группы.
            - Установление иерархии и распределения ролей (кураторы, кладмены, операторы – все анонимны).
            - Разграничение со ст. 228.1 УК РФ, совершенной группой лиц по предварительному сговору или ОПГ.
            - Применение норм о соучастии в условиях анонимности.
    - **Глава 3. Предложения по совершенствованию правоприменения и (возможно) законодательства.**
        - Рекомендации для следователей: использование цифровой криминалистики, анализ трафика, работа с провайдерами, международное сотрудничество.
        - Возможные изменения в УПК (касательно электронных доказательств) или методические рекомендации ВС РФ.
3. **Заключение:**
    - Основные выводы о сложностях.
    - Краткое изложение предложений.
    - Перспективы борьбы с онлайн-наркосообществами.
4. **Список литературы и источников.**

(Данный пример схематичен и требует глубокой проработки каждой части)

3. ПРОВЕРКА ПРАКТИЧЕСКИХ ЗАДАНИЙ, ВЫПОЛНЕННЫХ ОБУЧАЮЩИМИСЯ

Проверка выполнения практических заданий будет осуществляться комплексно:

1. **Текущий контроль на занятиях:**
    - Активность участия в обсуждениях, качество устных ответов, аргументированность позиции.
    - Оценка решений кейсов и выполнения аналитических/синтетических заданий в малых группах (с последующим представлением результатов и их обсуждением).
    - Моя задача – не просто поставить оценку, а помочь вам разобраться в сложных моментах, скорректировать неточности.
2. **Проверка мини-проекта:**
    - Оценивается как содержание представленной на занятии презентации, так и итоговый письменный текст мини-проекта.

Шкала оценивания (классическая 5-балльная):

- **"Отлично" (5 баллов):**
    - Демонстрирует глубокое и всестороннее понимание материала, свободное оперирование юридическими терминами.

- Безошибочно и аргументированно решает практические задачи (кейсы), точно квалифицирует деяния.
- Способен к глубокому анализу, выявлению неявных связей, формулированию оригинальных и обоснованных выводов.
- Предлагает конструктивные, юридически грамотные и творческие решения (в заданиях на синтез и в мини-проекте).
- Активно участвует в дискуссиях, четко излагает свою позицию.

- **"Хорошо" (4 балла):**
  - В целом правильно понимает материал, но может допускать незначительные неточности в определениях или трактовках.
  - Правильно решает практические задачи, но может испытывать затруднения в аргументации отдельных аспектов или допускать несущественные ошибки в квалификации, которые самостоятельно исправляет.
  - Способен к анализу, но выводы могут быть не всегда достаточно глубокими или оригинальными.
  - Предлагает дельные решения, но они могут требовать некоторой доработки.
  - Участвует в обсуждениях, но не всегда достаточно активно или аргументированно.
- **"Удовлетворительно" (3 балла):**
  - Имеет общее представление о теме, но допускает существенные неточности или пробелы в знаниях.
  - Затрудняется с решением практических задач, допускает ошибки в квалификации, требующие помощи преподавателя.
  - Анализ поверхностный, выводы недостаточно обоснованы.
  - Предложения по синтезу носят общий характер или недостаточно проработаны.
  - Пассивен в обсуждениях или испытывает трудности с формулированием мыслей.
- **"Неудовлетворительно" (2 балла):**
  - Демонстрирует отсутствие понимания основных положений темы.
  - Не способен решить практические задачи или дает неверные ответы.
  - Аналитические и синтетические навыки не развиты.
  - Не участвует в работе группы или не может сформулировать свою позицию.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДАННОЙ ТЕМЕ (ПОСЛЕАУДИТОРНОЙ)

1. **Глубокое изучение Постановлений Пленума ВС РФ:**

- ППВС РФ от 15.06.2006 N 14 "О судебной практике по делам о преступлениях, связанных с наркотическими средствами..." (в части использования ИТС).
- ППВС РФ от 09.07.2013 N 24 "О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях" (по аналогии для понимания квалификации посредничества, если применимо к некоторым схемам).
- Иные релевантные разъяснения и обзоры судебной практики.

2. **Анализ судебной практики:**
   - Самостоятельно подберите и проанализируйте 3-5 вступивших в законную силу приговоров (или апелляционных/кассационных определений) последних 2-3 лет по каждой из рассмотренных на занятиях категорий преступлений (наркотики через ИТ, организация проституции через ИТ, распространение порнографии через ИТ, треш-стримы, если есть практика). Обратите внимание на доказательственную базу, аргументацию суда, проблемы квалификации.
3. **Написание эссе (на выбор, объем 3-5 страниц):**
   - "Этико-правовые дилеммы криминализации/декриминализации оборота порнографии в цифровом обществе."
   - "Перспективы использования искусственного интеллекта в совершении и расследовании преступлений против общественной нравственности."
   - "Свобода слова vs. защита от деструктивного контента: поиск баланса на примере "треш-стримов"."

СПИСОК ВОПРОСОВ ДЛЯ САМОКОНТРОЛЯ

1. Каковы ключевые особенности бесконтактного сбыта наркотиков с использованием ИТ? Какие роли типичны для таких преступных схем?
2. В чем заключаются основные проблемы квалификации действий организаторов и участников онлайн-наркомаркетплейсов?
3. Как ИТ изменили рынок проституции? Какие новые риски и возможности это создало для вовлеченных лиц?
4. Какие составы УК РФ могут быть применены к деятельности "маркетплейсов" интим-услуг и онлайн-рекрутеров? В чем сложность доказывания?
5. Каково текущее состояние правового регулирования оборота порнографии в РФ? Аргументы "за" и "против" декриминализации "обычной" порнографии.
6. Что такое "дипфейки" и "порноместь"? Какие статьи УК РФ могут применяться к этим деяниям и каковы проблемы правоприменения?
7. Дайте определение "веб-каму" и "дикпикам". Почему эти явления вызывают сложности в правовой оценке?

8. Сравните российское и зарубежное законодательство в части ответственности за нежелательную рассылку интимных фото.
9. Что такое "треш-стримы"? Почему многие действия их участников остаются безнаказанными или влекут лишь административную ответственность?
10. Какие изменения в УК РФ могли бы повысить эффективность борьбы с "треш-стримами"?
11. Каким образом деструктивные организации используют ИТ в своей деятельности?
12. Какие элементы состава преступления (объект, объективная сторона, субъект, субъективная сторона) вызывают наибольшие сложности при квалификации преступлений против здоровья и нравственности, совершаемых с применением ИТ?
13. Какие методы толкования уголовного закона наиболее актуальны при анализе киберпреступлений в рассматриваемой сфере?
14. С какими проблемами сталкиваются правоохранительные органы при сборе и фиксации электронных доказательств по делам данной категории?
15. В чем заключается специфика применения норм о соучастии к преступлениям, совершаемым в анонимной онлайн-среде?

4. Текущий контроль успеваемости по теме № 5

Текущий контроль успеваемости проводится в форме выполнения мини-проекта.

Шкала и критерии оценивания приведены в оценочных средствах по дисциплине «Преступления в сфере высоких технологий» для данной ОПОП ВО, которые размещены на официальном сайте университета по ссылке https://swsu.ru/sveden/education/eduop/.

БИБЛИОГРАФИЧЕКИЙ СПИСОК

1. Уголовное право России. Общая часть : учебное пособие : [для студентов юридич. вузов всех уровней подготовки, аспирантов, преподавателей, научных работников] / Юго-Зап. гос. ун-т ; под общ. ред. А. А. Гребенькова. - 3-е изд., перераб. и доп. - Курск : ЮЗГУ, 2025. - 454 с. - ISBN 978-5-7681-1561-6 : 840.00 р. - Текст : непосредственный.
2. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва ; Берлин : Директ-Медиа, 2020. - 271 с. : табл. - URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 24.04.2025) . - Режим доступа: по подписке. - Библиогр. в кн. - ISBN 978-5-4499-0496-6 : Б. ц. - Текст : электронный.
3. Минин, А. Я. Актуальные проблемы цифрового права : учебное пособие для магистрантов и бакалавриата / А. Я. Минин. - Москва : Московский

педагогический гос. ун-т, 2021. - 132 с. - URL: http://www.iprbookshop.ru/115549 (дата обращения: 26.02.2022) . - Режим доступа: по подписке. - ISBN 978-5-4263-0984-5 : Б. ц. - Текст : электронный.

4. Алауханов, Е. О. Криминология : учебник / Е. О. Алауханов. - Санкт-Петербург : Юридический центр Пресс, 2024. - 608 с. - URL: http://www.iprbookshop.ru/137021 (дата обращения: 20.03.2025) . - Режим доступа: по подписке. - ISBN 978-5-94201-648-7 : Б. ц. - Текст : электронный.
5. Криминология : учебник / Г. А. Аванесов, Е. А. Антонян, С. В. Иванцов [и др.] ; под науч. ред. Г. А. Аванесова, Е. А. Антонян ; под общ. ред. З. Б. Соктоева, С. В. Иванцова. - 8-е изд., перераб. и доп. - Москва : Юнити-Дана, 2023. - 448 с. - URL: https://biblioclub.ru/index.php?page=book&id=712708 (дата обращения: 20.03.2025) . - Режим доступа: по подписке. - ISBN 978-5-238-03635-9 : Б. ц. - Текст : электронный.
6. Уголовное право России. Части Общая и Особенная : учебник для студентов бакалавриата и магистратуры / под ред. А. И. Рарога. - Изд. 10-е, перераб. и доп. - Москва : Проспект, 2020. - 944 с. - ISBN 978-5-392-30018-1 : 936.00 р. - Текст : непосредственный.