Федеральное государственное казенное
образовательное учреждение высшего образования
«Университет прокуратуры Российской Федерации»

Дальневосточный юридический институт (филиал)

Кафедра уголовно-правовых дисциплин

УТВЕРЖДЕН
на совместном заседании
кафедр
07.06.2023, протокол № 10
Заведующий кафедрой
Н.Н. Загвоздкин

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

Противодействие киберпреступности

Специальность 40.05.04 Судебная и прокурорская деятельность

Уровень профессионального образования
высшее образование - специалитет

Специализация
Прокурорская деятельность

Год начала подготовки – 2023

Очная форма обучения

Владивосток, 2023

Фонд оценочных средств по учебной дисциплине «Противодействие киберпреступности» обсужден и одобрен на совместном заседании кафедр Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации от 07.06.2023, протокол № 10.

Автор-составитель:

Побегайло А.Э. – доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, кандидат юридических наук

Фонд оценочных средств по учебной дисциплине «Противодействие киберпреступности» подготовлен в соответствии с требованиями федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.04 Судебная и прокурорская деятельность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 18.08.2020 № 1058.

СОДЕРЖАНИЕ

Стр.

1. Паспорт фонда оценочных средств ……. 4
2. Фонд оценочных средств для проведения текущего контроля обучающихся по дисциплине ..……. 5
3. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине ……. 26

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ «ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ»

№ п/п	Контролируемые разделы (темы) дисциплины	Код компетенции	Код индикатора достижения компетенции	Наименование оценочного средства
1.	Понятие киберпреступности	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
2.	История зарождения и современное состояние киберпреступности в РФ и иностранных государствах	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
3.	Преступления в сфере компьютерной информации как вид киберпреступлений	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
4.	Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
5.	Криминологическая характеристика киберпреступности и основные проблемы борьбы с ней	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
6.	Некоторые вопросы, связанные с расследованием киберпреступлений	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
7.	Соотношение уголовного, административного и гражданского права в вопросах охраны информации	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету
8.	Международно-правовой аспект борьбы с киберпреступностью	ПК-2	ПК–3.5, ПК–2.3, ПК–2.4	реферат; практические задачи; тестовые задания; вопросы к зачету

2. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Для проведения текущего контроля обучающихся по дисциплине «Противодействие киберпреступности» используются следующие оценочные средства:

1. реферат;
2. практические задачи;
3. тестовые задания;
4. контрольные работы.

2.1. Тематика рефератов

Тема 1. Понятие киберпреступности

1. Основные подходы к определению понятия «киберпреступность» и смежных понятий в правовой науке иностранных государств.
2. Основные подходы к определению понятия «киберпреступность» и смежных понятий в правовой науке современной России.

Тема 2. История зарождения и современное состояние киберпреступности в РФ и иностранных государствах

1. Современное состояние киберпреступности в Российской Федерации и мире – основные тенденции развития.
2. Киберпреступность в исторической перспективе.
3. Причины и условия возникновения киберпреступлений.
4. Современная структура, динамика, и общее состояние киберпреступности.
5. Киберпреступность: прогноз развития.
6. Международный характер киберпреступности.

Тема 3. Преступления в сфере компьютерной информации как вид киберпреступлений

1. Неправомерный доступ к компьютерной информации – проблемы квалификации.
2. Основные проблемные аспекты квалификации создания, использования и распространения вредоносных компьютерных программ.
3. Понятие «вредоносной программы» как средства совершения преступления.
4. «Иная компьютерная информация» как средство совершения преступления.
5. Вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие, особенности конструкции состава, вопросы квалификации.

Тема 4. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий

1. Информация как предмет преступления.
2. Кибернетические (цифровые) способы совершения преступлений как критерий квалификации.
3. Основные направления борьбы с распространением детской порнографии в сети Интернет.
4. Проблемы противодействия экстремизму в сети Интернет.
5. Мошенничество, совершенное с использованием платежных карт.
6. Расследование краж финансовых средств из электронных банковских сетей.
7. Кибертерроризм – определение, его предмет и способы совершения.
8. Проблемы расследования случаев мошенничества в сфере компьютерной информации.
9. Нарушение коммерческой тайны, совершенное с использованием киберсредств.
10. Нарушение личной тайны, совершенное с использованием киберсредств.

Тема 5. Основные проблемы борьбы с киберпреступностью

1. Транснациональный характер киберпреступности как актуальная проблема борьбы с нею.
2. Основные проблемы законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.
3. Основные проблемы механизмов взаимодействия правоохранительных и судебных органов разных стран.
4. Основные технические проблемы борьбы с киберпреступностью.
5. «Анонимность» в информационно-телекоммуникационных сетях как фактор развития правового нигилизма.
6. Основные аспекты сетевой культуры и менталитета, выступающие как поведенческие детерминанты преступности.
7. Незаконное использование криптовалют и средств электронных платежей как криминологическая проблема.
8. Влияние на преступность и вопросы криминализации незаконного использования «глубоких сетей» и их торговых площадок.

Тема 6. Некоторые вопросы, связанные с расследованием киберпреступлений

1. Техника, тактика и методика расследования компьютерных преступлений.

2. Техника, тактика и методика расследования преступлений, совершенных с использованием киберсредств и способов.

3. Отдельные моменты уголовно-процессуального характера в расследовании киберпреступлений.

4. Наиболее распространенные ошибки, допускаемые при расследовании и раскрытии киберпреступлений.

Тема 7. Соотношение уголовного, административного и гражданского права в вопросах охраны информации

1. Соотношение уголовного, административного и гражданского права в вопросах охраны интеллектуальной собственности.

2. Важность разграничения полномочий между уголовным и гражданским правом в аспекте защиты общественных отношений информационного характера.

Тема 8. Международно-правовой аспект борьбы с киберпреступностью

1. Основные международно-правовые договоры, регулирующие расследование киберпреступлений.

2. Международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними, их полномочия.

3. Подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений.

4. Вопросы разграничения юрисдикции при расследовании киберпреступлений.

Требования к рефератам

Реферат в учебном процессе представляет собой краткое изложение в письменном виде или в форме публичного доклада содержания научного труда или трудов специалистов по избранной теме, обзор литературы определенного направления.

Структура реферата включает следующие обязательные части: титульный лист; содержание (оглавление); введение; основная часть (раскрывается сущность выбранной темы); заключение; список использованной литературы.

Реферат должен быть правильно и аккуратно оформлен. Текст реферата (рукописный или в компьютерном исполнении) должен быть разборчивым, без стилистических и грамматических ошибок. Примерный объем реферата составляет 15–25 машинописных страниц.

Текст реферата должен раскрывать тему, обладать цельностью и связностью. Раскрытие темы предполагает, что в тексте реферата излагаются относящиеся к теме материалы и предлагаются пути решения содержащейся в контексте проблемы. Связность текста предполагает смысловую

соотносительность отдельных компонентов, а цельность – смысловую законченность текста.

Сокращение слов в тексте не допускается. Исключения составляют общеизвестные сокращения и аббревиатуры.

Во введении раскрываются цели и задачи, стоящие перед автором, объект и предмет изучения, дается общая характеристика использованным источникам. Объем введения не должен превышать 2-3 страницы.

В основной части реферата рассматриваются вопросы, раскрывающие поставленную проблему. Если при подборе материала студент сталкивается с тем, что в литературе нет единой точки зрения на рассматриваемую проблему, то нужно привести основные, наиболее интересные точки зрения разных авторов и дать им свою оценку.

Заголовки разделов и подразделов печатаются без абзацного отступа, прописными буквами, без точки в конце, без подчеркивания, по центру. Если заголовок состоит из двух предложений, их разделяют точкой.

Статистический, цифровой материал должен обосновывать и иллюстрировать мнения и выводы автора. Не следует перегружать реферат цифрами, статистическими выкладками (при необходимости их можно поместить в приложении), так как это отвлекает от понимания главных узлов темы и связи между ними. В части реферата необходимо достаточно полно и убедительно раскрыть все пункты плана, сохраняя логическую связь между ними и последовательность перехода от одного к другому. Каждый раздел заканчивается кратким выводом.

В заключении реферата должны быть аргументированные, т.е. обоснованные выводы и показано, насколько решены поставленные задачи. Здесь обобщаются изложенные в основной части материалы, формулируются общие выводы, указывается, что нового лично для себя вынес автор реферата из работы над ним. Делая выводы, необходимо учитывать различные опубликованные точки зрения на изложенную в работе проблему, сопоставить их и отметить, какая из них больше импонирует автору реферата.

В реферате, в частности, во введении и заключении, необходимо излагать личное отношение автора к раскрываемым вопросам. Заключение по объему, как правило, не должно превышать введения.

Список источников следует за заключением и оформляется с новой страницы. Список использованной литературы призван показать научную, теоретическую и практическую базу проведенного исследования.

Рекомендуемое количество использованной литературы для письменных работ для текущего контроля – не менее 5 и не более 50 литературных источников, нормативных правовых документов и иных источников.

Все указанные в тексте авторы и их работы, а также процитированные труды должны быть включены в этот список.

Критерии оценки:

оценка *«зачтено»* выставляется, если реферат соответствует установленным требованиям, и в рамках своей письменной работы студент продемонстрировал:

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; уголовно-правового понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за них; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; соотношения отраслей права в вопросах охраны информации; комплекса нормативных правовых актов, касающегося правоотношений в сфере охраны цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации;

– *умения*: осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по предупреждению и борьбе с киберпреступлениями; осуществлять правильную уголовно-правовую квалификацию киберпреступлений; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам борьбы с киберпреступностью); разрабатывать нормативные правовые акты в сфере борьбы с киберпреступностью; применять на практике нормативные правовые акты материального и процессуального права, их нормы, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности,

– *навыки* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере борьбы с киберпреступностью.

оценка *«не зачтено»* выставляется, если реферат не соответствует установленным требованиям, и в рамках своей письменной работы студент не продемонстрировал владение указанными знаниями, умениями и навыками.

2.2. Практические задачи

Тема 3. Преступления в сфере компьютерной информации как вид киберпреступлений.

1. Сорокин П.А., будучи работником электростанции ТЭЦ-21 г. Москвы, вступив в преступный сговор с группировкой хакеров «Орлы демократии», базирующейся в США, за вознаграждение тайно пронес на территорию предприятия USB-flash накопитель с вредоносным программным обеспечением. Сорокин вставил накопитель в один из компьютеров сети, в результате чего система была заражена вредоносной программой, могущей частично перехватывать на себя управление частью ключевых узлов станции.

Квалифицируйте содеянное Сорокиным П.А. и «Орлами демократии» соответственно. Какие следственные действия необходимо будет необходимо предпринять следственно-оперативной группе при расследовании данного деяния?

2. ООО «Технический Прогресс» оказывало услуги юридическим и частным лицам по установлению программного обеспечения (различных версий операционных систем Windows, офисных пакетов, программ специализированного назначения (Autodesk AutoCAD, Autodesk 3D Max, Adobe Photoshop и др.). При этом все версии, устанавливаемые данной фирмой на компьютеры заказчиков, были нелицензионными. Помимо этого, сотрудниками фирмы при установке использовались программы взлома защиты вышеуказанного ПО.

Квалифицируйте данные действия. Определите, кто будет нести ответственность за их совершение.

3. 14-летний учащийся 9-го класса средней школы, Петров П.В., написал компьютерный вирус, который сам распространял на различных Интернет-ресурсах под видом программы для обхода защиты нескольких компьютерных игр.

Квалифицируйте данное деяние. Будет ли Петров нести уголовную ответственность за него?

4. Соколов М.Ф. и Зубров И.И. совместно создали компьютерную программу, предназначенную для т.н. «майнинга» – математического вычисления hash-последовательностей. Данная программа запускалась втайне от пользователя и использовала системные ресурсы компьютера для вычислений без его ведома. Злоумышленники распространяли программу под видом программ-взломщиков защиты от копирования компьютерных игр. Добытая таким образом криптовалюта поступала на т.н. «кошельки», принадлежащие Соколову и Зуброву.

Квалифицируйте содеянное Соколовым и Зубровым.

5. Гришина Г.Д., работающая уборщицей в консалтинговой фирме «ГенриПитерс», в ходе проведения очередной уборки случайно задела кабель питания системы охлаждения серверной комнаты. В результате наступившего перегрева, несколько серверов вышли из строя. Часть информации, содержащейся на них, не поддавалась восстановлению. Это повлекло значительные финансовые убытки. Руководство фирмы обратилось в районное УВД с требованием возбудить против Гришиной уголовное дело по ч. 1 ст. 274 УК РФ.

Правомерны ли требования фирмы «ГенриПитерс»? Квалифицируйте содеянное Гришиной.

6. Захаров К.Л. создал веб-страницу, на которой выкладывал портативные версии различных компьютерных программ с открытым кодом. В дистрибутивы данных программ, втайне от пользователей, он внедрил троянскую программу Win32.Nimnul.a, с помощью которой получал контроль над зараженными компьютерами.

Являются ли его действия уголовным преступлением? Если да, то какое подразделение правоохранительных органов должно принять меры по выявлению данного преступления, и какие конкретные действия они должны будут совершить?

7. Константинов М.Н. написал исходный код троянской программы и выложил на свой сайт в свободный доступ. Саму программу он не компилировал. Используя данный исходный код, Максимов Н.О. произвел его компиляцию и создал исполняемый файл, который распространил в файлообменных сетях.

Квалифицируйте действия Константинова и Максимова.

Тема 4. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий.

1. Иванов И.А. разместил на анонимной доске объявлений ссылку на ролик порнографического содержания с участвуем заведомо несовершеннолетних.

Какое подразделение правоохранительных органов должно принять меры по выявлению данного преступления, и какие конкретные действия они должны будут совершить?

2. Жариков А.О., Семенов М.А., Кирюк М.М. и несколько неустановленных следствием лиц, организовали в «глубокой сети» торговую площадку «Ситцевая дорога», которая позволяла продавцам анонимно предлагать любой товар, включая оружие и наркотики, а покупателям – анонимно их оплачивать с помощью криптовалют. Эти же лица проверяли работу продавцов, в случае невыполнения ими своих обязательств штрафовали, в случае неоднократных действий по обману покупателей –

закрывали недобросовестный магазин. С каждой сделки, включая незаконные, Жарикову, Семенову, Кирюку и неустановленным лицам автоматически отчислялся процент.

Квалифицируйте содеянное Жариковым, Семеновым и Кирюком. Каким образом следствию возможно идентифицировать неустановленных лиц? Ответ обоснуйте.

3. Морозов В.С., 17-летний учащийся колледжа, путем использования массово рассылаемых фишинговых электронных сообщений похитил данные учетных записей массовой многопользовательской игры «Прекрасный мир», после чего в каждой похищенной учетной записи изменил данные, касающиеся имен пользователей и их электронных адресов, переоформив на несуществующих лиц. После этих действий, Морозов стал продавать эти учетные записи по договорной цене, изменяющейся в зависимости от содержащихся в них персонажей и виртуальных вещей.

Квалифицируйте действия Морозова. Ответ обоснуйте.

4. Сидоров С.Г., по мотивам мести своей бывшей сожительнице, Афанасьевой А.Б., используя известный ему пароль к учетной записи Афанасьевой в социальной сети, распространил в свободный доступ фотографии интимного содержания и иные личные данные, находившиеся в режиме закрытого доступа.

Являются ли его действия преступлением? Если да, то квалифицируйте данное деяние.

5. Березин Б.В., сотрудник коммерческого банка «Эпсилон-банк», решил доработать межбанковский договор по вопросам кредитования вне рабочего места, по причине недостатка времени. Он переписал данные на флэш-накопитель и продолжил работать с ними на своем домашнем компьютере. Служба безопасности конкурентов, банка «ВТФ12», осуществлявшая слежение за его компьютером, смогла завладеть данными сведеньями и использовать в свою пользу, в связи с чем «Эпсилон-банк» понес крупные убытки.

Являются ли действия Березина Б.В. преступлением? Если да, то квалифицируйте данное деяние.

6. Васильев В.Г. рассылал фальшивые электронные сообщения от лица фирмы «Арена-Два», являющейся разработчиком крупной многопользовательской компьютерной игры. В них он уведомлял пользователей, что в целях безопасности они должны изменить имя и пароль своей учетной записи. В письме содержалась ссылка на сайт, сделанный самим Васильевым, который практически полностью копировал дизайн сайта многопользовательской игры. Полученные таким образом имена пользователей и пароли, Васильев использовал для получения сведений о платежных картах пользователей, с целью хищения с них средств.

Квалифицируйте данные действия.

7. Новиков А.А., действуя под псевдонимом «АлыйКот», создал в социальной сети Вконтакте группу, в рамках которой под видом выполнения различных добровольных заданий – «квестов», втягивал подростков в нанесение себе телесных повреждений, убеждал в существовании иных миров, в которые они смогут попасть, выполняя его поручения, и, по достижении определенного уровня в организованной ими «игре», высылал задания, наводящие подростков на мысли о самоубийстве. При этом прямых угроз ни подросткам, ни их родным и близким Новиков не высказывал.

Квалифицируйте содеянное им. Какие действия необходимо выполнить следствию для установления всех потерпевших от действий Новикова и иных значимых обстоятельств по делу?

8. Дмитриев Д.Е, действуя под псевдонимом «Доброслав79», в течении длительного времени оставлял в социальных сетях сообщения оскорбительного содержания, направленные на разжигание национальной розни.

Являются ли его действия уголовным преступлением? Если да, то какое подразделение правоохранительных органов должно принять меры по выявлению данного преступления, и какие конкретные действия они должны будут совершить?

9. Емельянов Е.З., по мотивам ревности угрожал убийством своей бывшей жене, Емельяновой Я.И. Угрозы были высказаны им под различными псевдонимами через социальные сети и форумы, которые посещала его бывшая супруга.

Являются ли его действия уголовным преступлением? Если да, то квалифицируйте данные деяния.

10. Алферов С.С., испытывая романтические чувства к своей одногруппнице, Шиловой С.А., путем обмана, под видом помощи по написанию реферата, установил на ее ноутбук троянскую программу, после чего начал собирать ее фотографии и видео, сделанные через веб-камеру зараженного устройства, без согласия последней. После того, как Шилова отказала ему в начале романтических отношений, действуя по мотивам мести, Алефров распространил фото Шиловой интимного характера, полученные им с помощью троянской программы, на анонимной доске объявлений.

Квалифицируйте содеянное Алферовым.

11. Жихарев И.К. произвел незаконную видеозапись американского кинофильма «Карателя» и выложил его на торрент-сайт.

Являются ли его действия преступными? Если да, то дайте им уголовно-правовую квалификацию.

12. Ильюшенко Л.М. и его сообщник из Голландии Клаас Янсен создали интернет-магазин, торгующий семенами запрещенных на территории РФ наркотических растений. Сам сайт интернет-магазина находился на сервере, расположенном в Украине. При этом семена растений, высыпавшиеся

заказчикам, не соответствовали описанию на интернет-странице и представляли собой семена декоративных растений.

Являются ли их действия преступными? Если да, то государство какой страны будет осуществлять расследование и к подследственности какого правоохранительного органа относятся данные деяния.

13. Лобанов Н.О распространил через публичные торрент-трэккеры нелицензионную программу «Autodesk AutoCAD Architecture 2017 Commercial New Multi-user ELD 3-Year Subscription with Basic Support», стоимость одного лицензионного экземпляра которой составляет примерно 229 000 руб. Следствие квалифицировало его действия по ч.2 ст.272 УК РФ.

Правильная ли это квалификация? Обоснуйте ответ.

Тема 6. Некоторые вопросы, связанные с расследованием киберпреступлений

1. По сообщению о наличии на сайте сетевой энциклопедии «Мурклоар» призывов к подрыву конституционного строя, сведений, разглашающих государственную тайну, а равно и наличия рецептов изготовления самодельных взрывных устройств, следственной группой ФСБ были изъяты сервера, на которых находились файлы данной сетевой энциклопедии.

Какие действия по проверке данного сообщения должен предпринять эксперт?

2. Неустановленная группа лиц, в т.н. «Темном Интернете», используя возможности анонимной маршутизации «TOR», создала преступную организацию, занимающуюся торговлей наркотиками. В группе существовала иерархия, четкое разделение ролей, и сравнительная анонимность. Руководители группы действовали через подставных лиц, нанимая пособников – гарантов сделок, бухгалтеров, а равно и непосредственных исполнителей – наркодиллеров и наркокурьеров.

Какие действия необходимо предпринять оперативным сотрудникам для оперативного внедрения? Какие технические ошибки могут быть ими допущены?

3. Студент одного из московских технических ВУЗов Синякин распространял через социальные сети программу-вымогателя WantToWeep. При заражении программа автоматически требовала у потерпевшего перевести определенную сумму в биткоинах на несколько кошельков. Хотя Синякин соблюдал анонимность в управлении программой-вымогателем, он похвастался одногруппникам, что скоро разбогатеет и один из них сообщил в полицию.

Какова подследственность такого деяния? Какие действия должны произвести следователь, эксперт и оперативные сотрудники при задержании и обыске? Каких ошибок необходимо избегать?

Критерии оценки:

оценка «*отлично*» выставляется, если студент: решил практическое задание, не допустив ошибок; аргументировано предложенную им уголовно-правовую оценку со ссылкой на уголовное законодательство, нормативные и доктринальные правила квалификации преступлений; правильно отразил ее результаты в формуле квалификации, продемонстрировал тем самым отличное владение:

– *знаниями*: законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; уголовно-правового понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за них; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; соотношения отраслей права в вопросах охраны информации; комплекса нормативных правовых актов, касающегося правоотношений в сфере охраны цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации;

– *умениями*: осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по предупреждению и борьбе с киберпреступлениями; осуществлять правильную уголовно-правовую квалификацию киберпреступлений; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам борьбы с киберпреступностью); разрабатывать нормативные правовые акты в сфере борьбы с киберпреступностью; применять на практике нормативные правовые акты материального и процессуального права, их нормы, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности,

– *навыками* проверки нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере борьбы с киберпреступностью.

оценка *«хорошо»* выставляется, если студент: правильно решил практическое задание, но допустил некоторые ошибки при мотивировке квалификации преступления либо при отражении ее результатов; допустил незначительные ошибки при ответах на дополнительные вопросы преподавателя или обучающихся, продемонстрировав тем самым владение вышеуказанными знаниями, умениями и навыками на хорошем уровне;

оценка *«удовлетворительно»* выставляется, если студент: в целом решил практическое задание, но допустил при этом некоторые ошибки; испытывал определенные затруднения при мотивировке квалификации или отражении ее результатов; допустил существенные ошибки при ответах на дополнительные вопросы преподавателя или обучающихся, продемонстрировав тем самым удовлетворительное владение вышеуказанными знаниями, умениями и навыками;

оценка *«неудовлетворительно»* выставляется, если: не решил практическое задание либо допустил грубые ошибки при его решении, продемонстрировав тем самым неудовлетворительное владение вышеуказанными знаниями, умениями и навыками.

2.3. Тестовые задания

1. Киберпреступность это:

а) массовое, социально-негативное уголовно-правовое явление, выражающиеся в самовоспроизводящейся системе преступлений, связанных с использованием информационно-телекоммуникационных технологий;

б) совокупность преступлений, предусмотренных главной 28 Уголовного кодекса Российской Федерации;

в) прикладная научная и учебная дисциплина, целью которой является разработка способов и методов борьбы с компьютерными преступлениями;

г) совокупность преступлений, при совершении которых использовались достижения кибернетики.

2. Информационно-телекоммуникационные технологии это:

а) технологии телевизионного и радиовещания;

б) технологии защиты, хранения и передачи информации;

в) технологии обеспечения общения людей;

г) технологии передачи данных в цифровом формате.

3. Что является объектом дисциплины «Противодействие киберпреступности»:

а) преступления, предусмотренные главой 28 Уголовного кодекса;

б) приемы и способы раскрытия и расследования компьютерных преступлений;

в) киберпреступность в узком смысле этого термина, а также совокупность иных преступлений, совершенных с помощью информационных технологий;

г) общественные отношения по охране и защите информации.

4. Большинство определений компьютерной преступности в российской правовой науке базируется на определении, данном в:

а) минимальном и Необязательном списках правонарушений, рекомендованном странам-участницам ЕС;

б) соглашении о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации;

в) соглашении о сотрудничестве государств - участников ООН в борьбе с преступлениями в сфере компьютерной информации;

г) кодексе преступлений против мира и безопасности человечества.

5. В Российской Федерации борьбу с компьютерными преступлениями и преступлениями, совершенными с использованием информационно-коммуникационных технологий, осуществляет:

а) управление «К» при Бюро специальных технических мероприятий МВД РФ;

б) отдел «К» МВД РФ;

в) следственные отделы Следственного комитета РФ;

г) управление оперативно-технических мероприятий ФСБ РФ.

6. Интернет это:

а) общая совокупность интернет-сайтов, содержащихся на различных серверах;

б) всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных;

в) система хранения цифровой информации;

г) система связи.

7. В США ведущей организацией по приему жалоб на интернет-преступность является:

а) ФБР США;

б) Министерство Юстиции США;

в) полиция каждого конкретного штата;

г) Центр жалоб на интернет-преступность.

8. Количество официально зарегистрированных преступлений, предусмотренных главой 28 УК РФ в России за каждый год первого десятилетия XX в. измерялось:

а) десятками;

б) сотнями;

в) тысячами;

г) миллионами.

9. Кибертерроризм это:

а) осуществление террористических действий с использованием компьютерных вирусов и иных высокотехнологичных средств, направленных на выведение из строя промышленных, военных и иных объектов;

б) физическое уничтожение компьютеров и их сетей на промышленных, военных и иных объектах;

в) подготовка к террористическим действиям и координация их с использованием электронных сетей;

г) публичное одобрение терроризма в социальных сетях.

10. Современное поколение компьютеров и компьютерных устройств называется и появилось:

а) четвертым, появилось в 1970-х. г.г.;

б) третьим, появилось в 1980-х г.г.;

в) пятым, появилось в 1990-х г.г.;

г) шестым, появилось в 2000-х г.г.

11. Киберпреступление это:

а) преступление, совершенное киборгами;

б) преступление, совершенное с использованием информационно-телекоммуникационных технологий;

в) преступление, состав которого предусмотрен статьями главы 28 УК РФ;

г) преступление, совершенное в сети Интернет.

12. Компьютерная информация это:

а) любые сведения и данные (информация), представленные в форме электрических сигналов, независимо от средств их хранения, приема и передачи;

б) информация, находящаяся на жестком диске компьютера;

в) информация, находящаяся на носителе, в цифровой форме, доступной для считывания компьютером или компьютерным устройством;

г) информация, находящаяся в сети Интернет.

13. Вредоносная компьютерная программа, в уголовно-правовом понимании понятия, это:

а) представленная в исполняемой форме совокупность команд, предназначенных для функционирования компьютеров и компьютерных устройств в целях получения определенного преступного результата;

б) программа, наносящая вред общественным отношениям;

в) исполняемый файл, повреждающий компьютер и компьютерные устройства;

г) программа, наносящая вред здоровью и развитию несовершеннолетних.

14. Фишинг – это:

а) рыбная ловля;

б) компьютерный вирус, выводящий на дисплей изображение в виде рыбы;

в) вредоносная программа-червь, «выуживающая» данные пользователей через незакрытые порты сетевого соединения;

г) вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, совершаемый путем обмана или злоупотребления доверием.

15. Отметьте правильные варианты: объективная сторона базового состава ст. 272 УК РФ включает в себя следующие альтернативные последствия:

а) уничтожение компьютерной информации;

б) дизассемблирование компьютерной информации;

в) трансфер компьютерной информации;

г) декомпилирование компьютерной информации;

д) стирание компьютерной информации;

е) блокирование компьютерной информации;
ж) дублирование компьютерной информации;
з) модификации компьютерной информации,
и) дополнение компьютерной информации;
к) копирование компьютерной информации;
л) тестирование компьютерной информации.

16. Отметьте правильные варианты: объективная сторона базового состава ст. 273 УК РФ состоит из следующих альтернативных действий:

а) создании вредоносных компьютерных программ и иной компьютерной информации;
б) компилировании вредоносных компьютерных программ и иной компьютерной информации;
в) распространении вредоносных компьютерных программ и иной компьютерной информации;
г) блокировании вредоносных компьютерных программ и иной компьютерной информации;
д) уничтожении вредоносных компьютерных программ и иной компьютерной информации;
е) использовании вредоносных компьютерных программ и иной компьютерной информации.

17. Отметьте правильные варианты: специальными целями базового состава ст. 273 УК РФ являются:

а) уничтожение компьютерной информации;
б) дублирование компьютерной информации;
в) дополнение компьютерной информации;
г) блокирование компьютерной информации;
д) модификация компьютерной информации;
е) декомпилирование компьютерной информации;
ж) дизассемблирование компьютерной информации;
з) копирование компьютерной информации;
и) нейтрализация средств защиты компьютерной информации;
к) освобождение компьютерной информации;
л) получение незаконной выгоды с использованием компьютерной информации.

18. Предметом преступления, предусмотренного ст. 274 УК РФ является:

а) информационно-телекоммуникационная сеть,
б) сеть TOR;
в) сеть ФИДО;
г) оконечное оборудование;
д) роутер;
е) системный блок;
ж) средства хранения охраняемой компьютерной информации;
з) средства обработки охраняемой компьютерной информации;

и) средства копирования охраняемой компьютерной информации;

к) средства модификации охраняемой компьютерной информации;

л) средства передачи охраняемой компьютерной информации.

19. Отметьте правильные варианты; в полномочия каких федеральных органов и учреждений входит защита информации:

а) Федеральная таможенная служба;

б) Федеральная служба судебных приставов;

в) Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;

г) Служба внешней разведки;

д) Федеральная служба безопасности;

е) Министерство образования и науки Российской Федерации;

ж) Министерство экономического развития Российской Федерации;

з) Министерство обороны Российской Федерации;

и) Федеральная служба по техническому и экспортному контролю;

к) Следственный комитет Российской Федерации;

л) Министерство труда и социальной защиты Российской Федерации;

м) Федеральная служба охраны Российской Федерации.

20. Субъектами критической информационной инфраструктуры Российской Федерации являются (отметьте правильные варианты):

а) государственные органы;

б) частные лица;

в) российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат локальные сети;

г) государственные учреждения;

д) российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы;

е) российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационно-телекоммуникационные сети;

ж) российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат Интернет-магазины;

з) российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности;

и) российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;

к) российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат социальные сети;

л) некоммерческие благотворительные организации.

Критерии оценки:

оценка «*зачтено*» выставляется, если студент правильно ответил более чем на 65 % тестовых заданий, продемонстрировав тем самым:

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; уголовно-правового понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за них; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; соотношения отраслей права в вопросах охраны информации; комплекса нормативных правовых актов, касающегося правоотношений в сфере охраны цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации;

– *умения*: осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по предупреждению и борьбе с киберпреступлениями; осуществлять правильную уголовно-правовую квалификацию киберпреступлений; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам борьбы с киберпреступностью); разрабатывать нормативные правовые акты в сфере борьбы с киберпреступностью; применять на практике нормативные правовые акты материального и процессуального права, их нормы, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности,

– *навыки* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере борьбы с киберпреступностью;

оценка *«не зачтено»* выставляется, если студент правильно ответил менее чем на 65 % тестовых заданий, продемонстрировав тем самым

недостаточное для зачета владение вышеуказанными знаниями, умениями, навыками.

2.4. Контрольные работы

Вариант 1

1. В чем заключается транснациональный характер киберпреступности, и как он влияет на раскрытие такого рода преступлений?
2. Каковы правила по разграничению юрисдикции при расследовании киберпреступлений, и в каких нормативных правовых актах они содержатся?

Вариант 2

1. Каков современный взгляд на киберпреступность в российской и иностранной правовых науках?
2. Каким образом возникло такое явление как киберпреступность?

Вариант 3

1. Каково современное состояние киберпреступности в РФ и основные тенденции развития?
2. Какие существуют подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений?

Вариант 4

1. Какие существуют международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними?
2. Какие вы можете назвать основные международно-правовые договоры, регулирующие расследование киберпреступлений?

Вариант 5

1. Какие существуют основные условия возникновения киберпреступлений?
2. Что такое кибертерроризм (определение, его предмет и способы совершения)?

Вариант 6

1. Какова современная структура, динамика, и общее состояние киберпреступности?
2. Что такое право интеллектуальной собственности, и какие нормативные акты его регулируют?

Вариант 7

1. Какие существуют научные прогнозы развития киберпреступности в ближайшем будущем?

2. Почему киберпреступность имеет столь ярко выраженный международный характер?

Вариант 8

1. Назовите основные проблемы квалификации неправомерного доступа к компьютерной информации.

2. Проанализируйте основные проблемные моменты уголовно-процессуального характера в расследовании киберпреступлений.

Вариант 9

1. Каковы наиболее распространенные ошибки, допускаемые при расследовании и раскрытии преступлений, связанных с неправомерным доступом к компьютерной информации?

2. Назовите основные виды мошенничества, связанного с кредитными картами, осуществляемого с применением высоких технологий.

Вариант 10

1. Какие существуют основные приемы и способы неправомерного доступа к компьютерной информации?

2. В чем заключаются основные проблемные аспекты действий оперативно-розыскного характера, связанных с расследованием киберпреступлений?

Вариант 11

1. Какие существуют основные проблемы технического характера, возникающие при расследовании уголовных дел, связанных с созданием, использованием и распространением вредоносных компьютерных программ?

2. Раскройте основные проблемы, связанные с несовершенством соответствующего законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.

Вариант 12

1. Каковы основные орудия и способы создания, использования и распространения вредоносных компьютерных программ?

2. Назовите и раскройте сущность основных приемов и рекомендаций техники, тактики и методики расследования компьютерных и сопряженных с ними преступлений.

Вариант 13

1. Назовите основные уголовно-процессуальные вопросы расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ.

2. Назовите основные пути совершенствования механизмов взаимодействия правоохранительных и судебных органов разных стран по вопросам расследования киберпреступлений и судебного разбирательства по ним.

Вариант 14

14. Назовите основные вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

15. В чем основные особенности информации как предмета преступления?

Вариант 15

1. В чем основные особенности состава преступления, связанного с нарушением коммерческой и личной тайны?

2. Каковы основные направления борьбы с распространением детской порнографии в сети Интернет?

Вариант 16

1. Какие существуют основные проблемы противодействия экстремизму в сети Интернет?

2. Какие существуют основные проблемы расследования случаев мошенничества, совершенных с помощью высоких технологий?

Вариант 17

1. Каковы основные способы нарушения авторских и смежных прав, совершаемые с использованием киберсредств, в чем заключаются основные проблемы квалификации таких деяний?

2. Каково значение правовой компаративистики в рамках развития российского законодательства, посвященного борьбе с киберпреступностью?

Вариант 18

1. Каковы основные особенности вовлечения несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов, чем обусловлены проблемы выявления таких деяний?

2. Перечислите и раскройте основные криминогенные фоновые явления киберпреступности.

Вариант 19

1. Дайте характеристику составу преступления, предусмотренному ст. 159.3 УК РФ «Мошенничество, совершенное с использованием платежных карт», указав его проблемные аспекты.

2. Каковы основные особенности нарушения изобретательских и патентных прав, совершаемых с использованием киберсредств.

Вариант 20

1. Дайте уголовно-правовую характеристику незаконного распространения объектов авторского права и смежных прав путем использования файлообменного протокола «торрент».

2. Каковы особенности незаконного сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, а также незаконных сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, совершаемых с использованием информационно-телекоммуникационных сетей и иных киберсредств?

Вариант 21

1. Дайте уголовно-правовую характеристику состава склонения к совершению самоубийства или содействия совершению самоубийства.

2. В чем заключаются основные вопросы разграничения составов, связанных с хищениями путем обмана или злоупотребления доверием, осуществляемыми с использованием информационно-телекоммуникационных сетей?

Вариант 22

1. Каковы основные особенности нарушения патентных и смежных прав, осуществляемых с использованием киберсредств, в чем заключаются основные проблемы квалификации таких деяний?

2. Назовите основные механизмы рецепции международных правовых норм, касающихся цифровых общественных отношений, в национальное законодательство.

Критерии оценки: работа выполняется в письменном виде:

оценка *«зачтено»* выставляется, если студент правильно ответил на оба вопроса варианта контрольной работы, продемонстрировав тем самым:

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; уголовно-правового понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за них; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; соотношения отраслей права в вопросах охраны информации; комплекса нормативных правовых актов, касающегося правоотношений в сфере охраны цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации;

– *умения*: осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по

предупреждению и борьбе с киберпреступлениями; осуществлять правильную уголовно-правовую квалификацию киберпреступлений; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам борьбы с киберпреступностью); разрабатывать нормативные правовые акты в сфере борьбы с киберпреступностью; применять на практике нормативные правовые акты материального и процессуального права, их нормы, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности;

– *навыки* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере борьбы с киберпреступностью;

оценка *«не зачтено»* выставляется, если студент не ответил на оба вопроса варианта контрольной работы, продемонстрировав тем самым уровень владения вышеуказанными знаниями, умениями и навыками недостаточный для зачета.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Изучение учебной дисциплины «Противодействие киберпреступности» завершается промежуточной аттестацией – зачетом в устной форме.

Билеты для сдачи зачета содержат 2 теоретических вопроса.

Перечень вопросов для подготовки к зачету

1. Предмет и метод учебной дисциплины «Противодействие киберпреступности».
2. Понятие киберпреступности в узком и расширительном толковании термина.
3. Основные определения термина «киберпреступность» в правовой науке современной России; вопросы соотношения с определением термина «компьютерная преступность».
4. Основные определения понятия «киберпреступность» в правовой науке западных иностранных государств.
5. Киберпреступность в исторической перспективе (зарождение киберпреступлений, их развитие и эволюция).

6. Современное состояние киберпреступности, ее уровень, структура и динамика.

7. Прогноз дальнейшего состояния киберпреступности.

8. Международный характер явления киберпреступности: причины и влияние на предотвращение киберпреступлений.

9. Неправомерный доступ к компьютерной информации (осуществление с помощью вредоносных программ; осуществление с помощью иных высокотехнологичных средств); преступные последствия данного деяния и его квалифицирующие признаки.

10. Создание, использование и распространение вредоносных компьютерных программ, их основные виды; квалифицирующие признаки данного деяния и вопросы определения момента его окончания.

11. «Вредоносная программа» как средство совершения преступления: понятие, виды, особенности квалификации.

12. «Иная компьютерная информация» как средство совершения преступления: понятие, виды, особенности квалификации.

13. Нейтрализация средств защиты компьютерной информации как специфическое деяние, способы и средства его совершения.

14. Вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

15. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие, особенности конструкции состава, вопросы квалификации.

16. Информация как предмет преступления.

17. Кибернетические (цифровые) способы совершения преступлений как критерий квалификации.

18. Наиболее опасные из современных видов вирусных программ, механизм их действия.

19. Троянские программы, их отличие от вирусов, механизм их действия.

20. Информация как предмет преступления.

21. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, осуществляемые с использованием информационно-телекоммуникационных технологий.

22. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, осуществляемые с использованием сети Интернет.

23. Разжигание национальной, классовой и иной ненависти и вражды, а равно унижение человеческого достоинства, осуществляемые с помощью киберсредств.

24. Угрозы убийством, осуществляемые с помощью информационно-телекоммуникационных технологий.

25. Кража финансовых средств из электронных банковских сетей и основные пути ее совершения. Кража финансовых средств граждан (физических лиц) из электронных банковских сетей и платежных систем: проблемы квалификации, основные пути совершения.

26. Мошенничество, совершенное с применением киберсредств (компьютерных программ, сетей, иных высокотехнологичных средств).

27. Спам (как средство совершения преступлений): понятие, общественная опасность, основные способы борьбы.

28. Нарушение коммерческой и личной тайны: основные составы, вопросы квалификации.

29. Незаконные организация и проведение азартных игр, совершаемые с использованием сети Интернет и иных информационно-телекоммуникационных сетей.

30. Манипулирование рынком, осуществляемое с использованием информационно-телекоммуникационных технологий.

31. Основные проблемные аспекты законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.

32. Вопросы взаимодействия правоохранительных и судебных органов разных стран в рамках борьбы с киберпреступностью.

33. Основные аспекты сетевой культуры и менталитета, выступающие как поведенческие детерминанты преступности. «Анонимность» в информационно-телекоммуникационных сетях как фактор развития правового нигилизма.

34. Незаконное использование криптовалют и средств электронных платежей как криминологическая проблема.

35. Влияние на преступность и вопросы криминализации незаконного использования «глубоких сетей» и их торговых площадок.

36. Техника, тактика и методика расследования компьютерных преступлений.

37. Техника, тактика и методика расследования преступлений, совершенных с использованием киберсредств и способов.

38. Основные проблемы технического характера, препятствующие расследованию киберпреступлений.

39. Некоторые вопросы оперативно-розыскной деятельности, связанной с киберпреступлениями.

40. Отдельные моменты уголовно-процессуального характера в расследовании киберпреступлений.

41. Наиболее распространенные ошибки, допускаемые при расследовании и раскрытии компьютерных преступлений.

42. Право интеллектуальной собственности и его связь с борьбой с киберпреступностью.

43. Важность разграничения полномочий между уголовным и гражданским правом в аспекте защиты общественных отношений информационного характера.

44. Основные международно-правовые акты, регулирующие вопросы международного взаимодействия по борьбе с киберпреступностью, включая вопросы расследования киберпреступлений.

45. Международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними.

46. Подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений.

47. Разграничение юрисдикции при расследовании киберпреступлений.

48. Доведение до самоубийства, совершенное с использованием сети «Интернет».

49. Клевета, осуществляемая с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

50. Нарушение неприкосновенности частной жизни, совершенное путем использования информационно-телекоммуникационных технологий. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенные с использованием киберсредств.

51. Нарушение авторских и смежных прав, совершенное с использованием киберсредств.

52. Вовлечение несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

53. Мошенничество, совершенное с использованием платежных карт, осуществляемое с применением кибертехнологий.

54. Неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.

55. Разжигание национальной, классовой и иной розни, угроза убийством, осуществляемые с помощью киберсредств.

56. Кибертерроризм – определение, его предмет и способы совершения.

57. Осуществление публичных призывов к осуществлению террористической деятельности или публичное оправдание терроризма, совершаемое с помощью информационно-телекоммуникационных технологий.

58. Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, совершаемые с использованием информационно-телекоммуникационных сетей и иных киберсредств.

59. Склонение к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети.

60. Организация деятельности, направленной на побуждение к совершению самоубийства.

61. Торговля людьми, совершаемая с использованием информационно-телекоммуникационных сетей.

62. Развратные действия, совершаемые путем использования ресурсов сети Интернет.

63. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации, осуществляемый через информационно-телекоммуникационные сети.

64. Нарушение изобретательских и патентных прав, совершенное с использованием информационно-телекоммуникационных технологий.

65. Мелкое хищение, совершенное лицом, подвергнутым административному наказанию, совершаемое с использованием информационно-телекоммуникационных сетей путем обмана или злоупотребления доверием.

66. Незаконная банковская деятельность, осуществляемая посредством использования информационно-телекоммуникационных сетей и иных киберсредств.

67. Неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.

68. Содействие террористической деятельности, осуществляемое с помощью сети Интернет и иных информационно-телекоммуникационных сетей.

69. Организация террористического сообщества или организации и участие в нем (ней), осуществляемые с использованием киберсредств.

70. Заведомо ложное сообщение об акте терроризма, совершаемое с использованием киберсредств.

71. Организация преступного сообщества (преступной организации) или участие в нем (ней), совершаемая путем использование информационно-телекоммуникационных сетей и ресурсов.

72. Организация массовых беспорядков, совершаемая с использованием Интернета и иных информационно-телекоммуникационных сетей

73. Незаконные приобретение, передача, сбыт оружия, его основных частей, боеприпасов, взрывных устройств или взрывчатых веществ, осуществляемая с использованием информационно-телекоммуникационных сетей и их ресурсов.

74. Склонение к потреблению наркотических средств, психотропных веществ или их аналогов, совершаемое с помощью Интернета и иных информационно-телекоммуникационных сетей.

75. Незаконный оборот сильнодействующих или ядовитых веществ, а равно новых потенциально опасных психоактивных веществ в целях сбыта, совершаемый с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

76. Незаконные изготовление и оборот порнографических материалов или предметов, совершаемые с использованием информационно-телекоммуникационных сетей.

Критерии оценки:

1. Оценка *«зачтено»* выставляется, если студент продемонстрировал овладение планируемыми компетенциями, ответил на теоретические вопросы, содержащиеся в билете, продемонстрировав:

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; уголовно-правового понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за них; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; соотношения отраслей права в вопросах охраны информации; комплекса нормативных правовых актов, касающегося правоотношений в сфере охраны цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации;

– *умения*: осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по предупреждению и борьбе с киберпреступлениями; осуществлять правильную уголовно-правовую квалификацию киберпреступлений; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам борьбы с киберпреступностью); разрабатывать нормативные правовые акты в сфере борьбы с киберпреступностью; применять на практике нормативные правовые акты материального и процессуального права, их нормы, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности;

– *навыки* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере борьбы с киберпреступностью.

2. Оценка *«не зачтено»* выставляется, если студент не ответил на теоретические вопросы, содержащиеся в билете, либо допустил грубые ошибки при ответе на теоретические вопросы, показав тем самым отсутствие вышеперечисленных знаний, умений, навыков.