

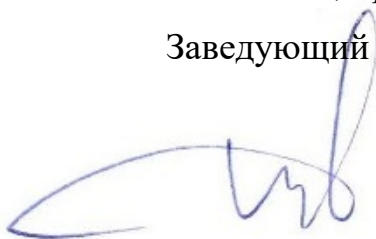
**Федеральное государственное казенное
образовательное учреждение высшего образования
«Университет прокуратуры Российской Федерации»**

Дальневосточный юридический институт (филиал)

УТВЕРЖДЕН

на совместном заседании кафедр
12.05.2026, протокол № 12

Заведующий кафедрой
В.Б. Хазизулин



**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 – 2026

Очная форма обучения

Владивосток, 2026

Фонд оценочных средств по учебной дисциплине «» обсужден и одобрен на совместном заседании кафедр Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации от 12.05.2026, протокол № 12, на заседании учебно-методического совета института 16.05.2026, протокол №1.

Авторы-составители:

Винокуров М.В., к.ю.н.
Гаврилов М.А., к.ю.н.
Гундериц Г.А., к.т.н., доцент
Ермолова Е.В.,
Побегайло А.Э., к.ю.н.
Попов А.Н., д.ю.н., профессор
Сыромля Л.Б., к.ю.н.

Фонд оценочных средств по учебной дисциплине «Практика и проблемы назначения уголовных наказаний» подготовлен в соответствии с требованиями федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.04 Судебная и прокурорская деятельность, утвержденного приказом Минобрнауки России от 18.08.2020 г. № 1058.

Предназначен для обучающихся Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации.

© Университет прокуратуры
Российской Федерации, 2026.
© Винокуров М.В., Гаврилов М.А.,
Гундериц Г.А., Ермолова Е.В., Побегайло
А.Э., Попов А.Н., Сыромля Л.Б.

Оглавление

1. Цель фонда оценочных средств.....	4
2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы	4
3. Уровни сформированности компетенций, шкала и критерии оценивания освоения дисциплины	7
4. Паспорт фонда оценочных средств по дисциплине «Противодействие киберпреступности».....	7
5. Оценочные средства по дисциплине «Противодействие киберпреступности».	10
<i>Перечень примерных вопросов для проведения устного опроса.....</i>	<i>10</i>
<i>Варианты докладов по темам:</i>	<i>15</i>
<i>Аудиторная контрольная работа по дисциплине «Противодействие киберпреступности» (Типовая)</i>	<i>18</i>
<i>Примеры практических задач</i>	<i>22</i>
6. Контрольно-измерительные материалы по дисциплине.....	30
<i>Примерный перечень вопросов для подготовки к зачету.....</i>	<i>30</i>
<i>Комплект задач для проведения экзамена</i>	<i>37</i>
<i>Образец билета к зачету.....</i>	<i>43</i>
<i>Шкала и критерии оценивания на зачете</i>	<i>43</i>

1. Цель фонда оценочных средств

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся по учебной дисциплине «Противодействие киберпреступности». Перечень видов оценочных средств соответствует рабочей программе учебной дисциплины.

Фонд оценочных средств включает контрольно-измерительные материалы для проведения текущего контроля и промежуточной аттестации, указанных в рабочей программе учебной дисциплины, а также критерии оценок (шкалу оценивания) к ним.

Структура и содержание заданий – задания разработаны в соответствии с рабочей программой учебной дисциплины «Противодействие киберпреступности».

В структурных подразделениях Университета прокуратуры Российской Федерации, в том числе в его институтах (филиалах) оценочные средства могут использоваться в рамках электронной информационно-образовательной среды с учётом действующих локальных нормативных правовых актов Университета и его институтов (филиалов).

2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и наименование компетенции	Код и наименование индикатора компетенции	Этап формирования	Предшествующий и последующий этапы (с указанием дисциплин)
ПК-2. Способен квалифицированно, юридически правильно толковать и применять нормы законодательства различных отраслей права при осуществлении прокурорской деятельности, в том числе в их системной связи.	ПК-2.3. Юридически правильно применяет нормы законодательства различных отраслей права при осуществлении уголовного преследования.	8 из 10 этапов	6 этап - Уголовный процесс 7 этап - Прокурорский надзор 8 этап -Криминалистика 8 этап - Квалификация преступлений 9 этап - Участие прокурора в судебных стадиях уголовного судопроизводства 8 этап - Противодействие киберпреступности 10 этап - Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)

	ПК-2.4 Юридически правильно применяет нормы законодательства, регламентирующие участие прокурора в рассмотрении дел судами	8 из 10 этапов	5,6 этап - Уголовный процесс 7,8 этап - Прокурорский надзор 9 этап - Участие прокурора в судебных стадиях уголовного судопроизводства 6,8, 10 этап - Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)
--	--	----------------	---

ПК-3. Способен выполнять должностные обязанности по обеспечению законности, защите прав и законных интересов граждан, организаций, охраняемых законом интересов общества и государства.	ПК-3.5. Осуществляет профилактику, предупреждение, пресечение преступлений и правонарушений, выявляет и устраняет причины и условия, способствующие их совершению.	8 из 10 этапов	7 этап - Криминология 7 этап - Юридическая психология 8 этап - Противодействие коррупции 9 этап - Прокурорский надзор за исполнением законов администрациями органов и учреждений, исполняющих наказание и назначаемые судом меры принудительного характера, администрациями мест содержания задержанных и заключенных под стражу 9 этап - Прокурорский надзор за исполнением законов на транспорте и в таможенной сфере 10 этап - Координация деятельности правоохранительных органов по борьбе с преступностью 10 этап - Прокурорский надзор за исполнением законов судебными приставами 10 этап - Производственная практика (практика по получению профессиональных умений и опыта профессиональной деятельности)
---	--	----------------	---

Основными этапами формирования указанных компетенций в процессе освоения образовательной программы являются последовательное изучение дисциплин направленных на формирование «одинаковых» компетенций. Этап формирования компетенций определяется местом дисциплины в образовательной программе (раздел 3 рабочей программы дисциплины). Изучение каждой дисциплины предполагает овладение обучающимися необходимыми знаниями, умениями и навыками, соотнесенными с

индикаторами достижения компетенции. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающимися.

Распределение компетенций (индикаторов достижения компетенций) по дисциплинам закреплено в Общей характеристике основной образовательной программы.

3. Уровни сформированности компетенций, шкала и критерии оценивания освоения дисциплины

<i>Уровни сформированности компетенций</i>	Пороговый	Базовый	Повышенный
<i>Шкала оценивания</i>	Оценка «зачтено»	Оценка «зачтено»	Оценка «зачтено»
<i>Критерии оценивания</i>	Компетенция сформирована. Демонстрируется недостаточный уровень самостоятельности практического навыка	Компетенция сформирована. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка	Компетенция сформирована. Демонстрируется высокий уровень самостоятельности, высокая адаптивность научных знаний и практического навыка

В качестве основного критерия оценивания освоения дисциплины обучающимся используется наличие сформированных компетенций (компетенции).

Положительная оценка по дисциплине может выставляться и при неполной сформированности компетенции (компетенций), если её (их) формирование предполагается продолжить в ходе изучения других дисциплин или прохождения практик (в соответствии с Матрицей формирования компетенций, представленной в Общей характеристике ООП).

4. Паспорт фонда оценочных средств по дисциплине «Противодействие киберпреступности»

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Вид контроля	Наименование оценочного средства и форма задания
1	Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика	ПК-2.3, ПК-2.4, ПК-3.5.	Текущий контроль	Задания в открытой форме: -перечень примерных вопросов для проведения

				устного опроса; -примерная тематика докладов;
2	Тема 2. Преступления в сфере компьютерной информации	ПК-2.3, ПК-2.4, ПК-3.5.	Текущий контроль	Задания в открытой форме: -перечень примерных вопросов для проведения устного опроса; - -практические задачи (ситуации); -примерная тематика докладов.
3	Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий	ПК-2.3, ПК-2.4, ПК-3.5.	Текущий контроль	Задания в открытой форме: -перечень примерных вопросов для проведения устного опроса; -перечень примерных вопросов для проведения дискуссии; -практические задачи (ситуации); -примерная тематика докладов.
4	Тема 4. Проблемы квалификации киберпреступлений	ПК-2.3, ПК-2.4, ПК-3.5.	Текущий контроль	Задания в открытой форме: -перечень примерных вопросов для проведения устного опроса; -практические задачи (ситуации); - примерное задание для письменной контрольной работы

5	Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе	ПК-2.3, ПК-2.4, ПК-3.5.	Текущий контроль	Задания в открытой форме: -перечень примерных вопросов для проведения устного опроса; -примерная тематика докладов; -практические задачи (ситуации);
6	Зачет	ПК-2.3, ПК-2.4, ПК-3.5.	Промежуточная аттестация	Примерный перечень вопросов для подготовки к зачету. Комплект задач для проведения зачета. Образец билета. Шкала и критерии оценивания.

ПК-2. Способен квалифицированно, юридически правильно толковать и применять нормы законодательства различных отраслей права при осуществлении прокурорской деятельности, в том числе в их системной связи.

ПК-2.3. Юридически правильно применяет нормы законодательства различных отраслей права при осуществлении уголовного преследования.

ПК-2.4. Применяет правовые нормы, регламентирующие участие прокурора в рассмотрении дел судами.

ПК-3. Способен выполнять должностные обязанности по обеспечению законности, защите прав и законных интересов граждан, организаций, охраняемых законом интересов общества и государства.

ПК-3.5. Осуществляет профилактику, предупреждение, пресечение преступлений и правонарушений, выявляет и устраняет причины и условия, способствующие их совершению.

Обучающийся знает: понятия, виды и состав киберпреступлений; уголовно-правовые нормы, устанавливающих ответственность за киберпреступления; соотношения отраслей права в вопросах охраны информации;

Обучающийся умеет: применять на практике нормативные правовые акты материального и процессуального права, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, надзора за их расследованием и раскрытием;

Обучающийся владеет навыками: по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы информационно-

телекоммуникационных технологий, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений.

5. Оценочные средства по дисциплине «Противодействие киберпреступности».

Перечень примерных вопросов для проведения устного опроса

Код формируемой компетенции (или ее части):
ПК-2.3, ПК-2.4, ПК-3.5.

Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика

Практическое занятие 1.

1. Дайте определение понятия и предмета дисциплины «Противодействие киберпреступности».
2. Основные методы изучения киберпреступности
3. Укажите систему и задачи дисциплины «Противодействие киберпреступности».
4. История развития информационно-телекоммуникационных технологий.
5. Основные этапы развития компьютерной техники.
6. Назовите основные этапы развития языков программирования и машинного обучения.
7. История развития информационно-телекоммуникационных сетей, включая сеть Интернет
8. Основные этапы разработки вредоносных компьютерных программ.
9. Назовите основные этапы зарождения и развития киберпреступности в исторической перспективе.

Практическое занятие 2.

1. Понятие киберпреступности.
2. Отражение понятия киберпреступность в российской и иностранной правовых науках.
3. Современное состояние киберпреступности в РФ и основные тенденции ее дальнейшего развития как массового, социально-негативного, уголовно-правового явления.
4. Основные условия и причины возникновения киберпреступлений.

5. Современные структура, динамика и общее состояние киберпреступности.
6. Прогноз развития киберпреступности
7. Международный характер киберпреступности
8. Основные проблемы в противодействии противодействия киберпреступности
9. Влияние сетевой псевдоанонимности и сетевой культура на киберпреступность

Тема 2. Преступления в сфере компьютерной информации

Практическое занятие 3.

1. Проблемы квалификации неправомерного доступа к компьютерной информации
2. Основные приемы и способы неправомерного доступа к компьютерной информации
3. Основные средства и способы создания, использования и распространения вредоносных компьютерных программ
4. Вопросы квалификации преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ

Практическое занятие 4.

1. Назовите основные вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
2. Назовите основные аспекты квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
3. Основные вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Практическое занятие 5.

1. Назовите основные проблемы квалификации нарушения правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования
2. Особенности информации как предмета преступления. Назовите основные аспекты использования киберсредств как средства и способа совершения преступления.
3. Назовите основные проблемы квалификации незаконного использования абонентского терминала пропуска трафика или виртуальной телефонной станции.

Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий

Практическое занятие 6.

1. Назовите преступления против жизни и здоровья, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

3. Назовите преступления против половой свободы и половой неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

4. Перечислите преступления против конституционных прав и свобод человека и гражданина, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

5. Преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Практическое занятие 7.

1. Назовите преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

3. Назовите преступления против общественной безопасности и общественного порядка, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

4. Преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

5. Перечислите преступления против основ конституционного строя и безопасности государства, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Практическое занятие 8.

1. Назовите преступления против государственной власти, интересов государственной службы, и службы местного самоуправления, совершаемые

посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Преступления против порядка управления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации

3. Назовите преступления против мира и безопасности человечества, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Тема 4. Проблемы квалификации киберпреступлений

Практическое занятие 9.

1. Особенности квалификации неправомерного доступа к компьютерной информации

2. Конкуренция неправомерного доступа к компьютерной информации и нарушения тайны переписки, телефонных переговоров, телеграфных и иных сообщений

3. Основные вопросы квалификации нарушения неприкосновенности частной жизни, совершаемой путем неправомерного доступа к компьютерной информации

4. Основные особенности квалификации создания, распространения и использования вредоносных компьютерных программ?

Практическое занятие 10.

1. Конкуренция составов неправомерного доступа к компьютерной информации и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

2. Проблемные аспекты нормативного определения критической информационной инфраструктуры Российской Федерации как предмета преступления

3. Основные проблемные аспекты определения момента начала и момента окончания киберпреступлений

4. Основные вопросы совокупности преступлений в сфере компьютерной информации от единого продолжаемого преступления?

Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе

Практическое занятие 11.

1. Назовите основные международно-правовые договоры, регулирующие расследование киберпреступлений.

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

3. Подразделения правоохранительных органов основных иностранных

государств, занимающихся расследованием киберпреступлений

4. Правила по разграничению юрисдикции при расследовании киберпреступлений и нормативные правовые акты, их содержащие.

Практическое занятие 12.

1. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.

2. Основные подходы стран БРИКС по противодействию киберпреступности

3. Роль стран ШОС в противодействии кибертерроризму

4. Меры по противодействию киберпреступности предпринимаются странами-участниками ЕАЭС

Критерии оценивания

Устный опрос на практическом занятии оценивается по следующим критериям: полнота и развернутость всех основных элементов, составляющих содержание вопроса; понимание сущности раскрываемого вопроса; правильность и корректность использования терминологического аппарата; умение связать абстрактные знания с конкретными явлениями, показать на примерах основные положения вопроса; понимание связей между различными элементами содержания вопроса, а также его взаимосвязей с другими темами дисциплины и материалом иных учебных дисциплин образовательной программы; логичность и аргументированность ответа; осознанность, самостоятельность мышления.

Шкала оценивания

Оценка *«отлично»* выставляется студенту, если он принимает активное участие в устном опросе; показывает высокий уровень знаний в сфере жилищного права; имеет представление об основных сложившихся на практике и (или) в доктрине подходах по рассматриваемому вопросу; аргументировано отстаивает выбранную позицию; ответ структурирован, выстроен в логической последовательности, изложен грамотным языком.

Оценка *«хорошо»* выставляется студенту, если он принимает участие в устном опросе; показывает достаточный уровень знаний жилищного права; имеет представление об отдельных сложившихся на практике и (или) в доктрине подходах по рассматриваемому вопросу; пытается высказать личную позицию; ответ структурирован, выстроен в логической последовательности, изложен грамотным языком; допущены отдельные неточности в изложении и аргументации.

Оценка «удовлетворительно» выставляется студенту, если он принимает участие в устном опросе; показывает средний уровень знаний жилищного права; имеет весьма несистематизированные, разрозненные представления о сложившихся на практике и (или) в доктрине подходах по рассматриваемому вопросу; допущены неточности в изложении и аргументации.

Оценка «неудовлетворительно» выставляется, если студент не участвует в устном опросе либо в ходе такого участия показывает низкий уровень знаний жилищного права; при ответе допущены существенные нарушения логики и последовательности изложения, грубые ошибки; речь неграмотная.

Варианты докладов по темам:

Код формируемой компетенции (или ее части):

ПК-2.3, ПК-2.4, ПК-3.5.

Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика.

1. Основные определения термина «киберпреступность» в правовой науке современной России.
2. Киберпреступность в исторической перспективе.
3. Криминологическая характеристика киберпреступности.
4. Транснациональный характер киберпреступности как один из основных проблемных аспектов борьбы с ней.
5. «Даркнет», «глубокие сети» и их торговые площадки – вопросы криминализации их незаконного использования и влияния на преступность.

Тема 2. Преступления в сфере компьютерной информации.

1. Неправомерный доступ к компьютерной информации
2. Незаконное использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные
3. Понятие персональных данных как предмета преступления
4. Создание, использование и распространение вредоносных компьютерных программ
5. Вирусы в исторической перспективе
6. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
7. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции
8. Организация деятельности по передаче абонентских номеров с нарушением требований законодательства Российской Федерации
9. Организация деятельности по передаче информации, необходимой для регистрации и (или) авторизации пользователя сети "Интернет" для получения доступа к функциональным возможностям информационного ресурса

Тема 3. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий.

1. Преступления против жизни и здоровья, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации

2. Преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации

3. Преступления против половой свободы и половой неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации. Развратные действия, совершаемые путем использования ресурсов сети Интернет.

4. Преступления против конституционных прав и свобод человека и гражданина, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

5. Преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

6. Преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

7. Преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

8. Преступления против общественной безопасности и общественного порядка, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

9. Преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

10. Преступления против основ конституционного строя и безопасности государства, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Тема 4. Проблемы квалификации киберпреступлений.

1. Особенности квалификации неправомерного доступа к компьютерной информации.

2. Особенности квалификации подделки, изготовления или оборота поддельных цифровых документов, соотношение со внесением несанкционированных изменений в государственные базы данных.

3. Нарушение неприкосновенности частной жизни, совершаемой путем неправомерного доступа к компьютерной информации: вопросы квалификации.

4. Особенности квалификации создания, распространения и использования вредоносных компьютерных программ.

5. Проблемы определения малозначительности создания, распространения и использования вредоносных компьютерных программ.

Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе.

1. Имплементация международно-правовых норм, регулирующих вопросы, связанные с цифровыми технологиями, информационно-телекоммуникационными сетями и смежными вопросами в национальное законодательство.

2. Вопросы гармонизации норм уголовного и уголовно-процессуального законодательства, касающихся криминализации киберпреступлений, их расследования и судебного разбирательства.

3. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.

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

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

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

7. Установление и разграничение юрисдикции при расследовании киберпреступлений, при затрагивании законных интересов граждан двух и более государств.

8. Основные подходы стран БРИКС по противодействию киберпреступности.

9. Роль стран ШОС в противодействии кибертерроризму.

10. Меры по противодействию киберпреступности стран-участниц ЕАЭС.

Аудиторная контрольная работа по дисциплине «Противодействие киберпреступности» (Типовая)

**Код формируемой компетенции (или ее части):
ПК-2.3, ПК-2.4, ПК-3.5.**

Вариант 1

Иностранный гражданин Ч., студент медицинского университета, поздно ночью проник в здание филиала коммерческого банка и похитил из сейфа различные документы, наличные деньги, а также несколько флэш-накопителей, предназначенных для работы с компьютером банка. Поскольку Ч. сам не разбирался в компьютерной технике, то он продал похищенные флэш-накопители своему знакомому К., который работал программистом в НИИ. Используя информацию, хранимую на флэш-накопителях, К. получил электронный доступ в банковский компьютер, в результате чего совершил хищение крупной суммы денег со счетов вкладчиков.

Решите вопрос об ответственности указанных в задаче лиц.

Вариант 2

Работник НИИ М. разработал компьютерный вирус, поражающий текстовую информацию на компьютере, и продемонстрировал возможности этой программы коллеге Г., который без разрешения автора переписал программу-вирус на свою флэш-карту. Перед увольнением из НИИ Г., желая отомстить своему начальнику, инфицировал его компьютер этим вирусом, что повлекло изменение первоначальной информации на этом компьютере.

Квалифицируйте действия М. и Г. Имеются ли в их действиях признаки состава преступления?

Шкала и критерии оценивания аудиторной контрольной работы

Критериями оценивания аудиторной контрольной работы являются:

- правильность ответа и решения задачи;
- полнота ответа и решения задачи;
- изложение нескольких теоретических подходов к освещаемой проблеме;
- полнота, последовательность, обоснованность изложенной позиции, в том числе подтвержденная ссылкой на правовые позиции Верховного Суда Российской Федерации, Конституционного суда Российской Федерации, иной судебной практики.

Оценка *«отлично»* выставляется, если студент правильно и полно решил задачу (дана правильная и полная квалификация (статья, часть, пункт УК РФ) в отношении всех фигурантов фабулы дела), а также продемонстрировал способность логично, аргументированно и ясно строить свой ответ со ссылками на материалы судебной практики.

Оценка *«хорошо»* выставляется, если студент в основном правильно решил задачу, допустив незначительную неполноту (дана правильная квалификация преступления в отношении всех фигурантов фабулы дела, однако

с установлением большинства квалифицирующих признаков, допустил неполноту или несущественные ошибки в изложении подходов к проблеме).

Оценка «удовлетворительно» выставляется, если студент в основном правильно решил задачу, допустив несущественную неполноту (дана правильная квалификация преступления в отношении большинства фигурантов фабулы дела, однако с установлением меньшинства квалифицирующих признаков или без оценки меньшинства преступлений, требующих дополнительной квалификации, без ответа в изложении подходов к проблеме, при частичном подтверждении ответа материалами судебной практики);

Оценка «неудовлетворительно» выставляется, если студент неправильно решил задачу либо допустил при ее решении существенную неполноту (дана правильная, но неполная квалификация преступления в отношении всех фигурантов фабулы дела без установления квалифицирующих признаков или без оценки большинства преступлений, требующих дополнительной квалификации; дана неправильная или неполная квалификация в отношении большинства фигурантов фабулы дела, сопровождаемая отсутствием ответа в изложении подходов к проблеме, без подтверждения материалами судебной практики).

Варианты аудиторных и домашних контрольных работ

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. В чем заключаются основные актуальные вопросы противодействию угрозам убийством в сети Интернет?

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. В чем состоят актуальные проблемы квалификации преступлений, совершенных с использованием Даркнет-ресурсов?

Вариант 9

1. Каковы существуют наиболее распространенные ошибки, допускаемые при расследовании и раскрытии преступлений, связанных с неправомерным доступом к компьютерной информации?
2. Назовите основные способы совершения мошенничества в сфере электронных средств платежа и проблемы его отграничения от смежных составов.

Вариант 10

1. Какие существуют основные приемы и способы неправомерного доступа к компьютерной информации?
2. Каковы основные проблемные вопросы квалификации преступлений, совершаемых с использованием криптовалют?

Вариант 11

1. Какие существуют проблемы квалификации склонения к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети?
2. Раскройте основные проблемы, связанные с несовершенством соответствующего законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.

Вариант 12

1. Каковы основные способы создания, использования и распространения вредоносных компьютерных программ?
2. Каковы проблемные аспекты квалификации развратных действий, совершаемых путем использования ресурсов сети Интернет?

Вариант 13

1. Охарактеризуйте основные проблемные аспекты квалификации нарушения неприкосновенности частной жизни, совершенного путем использования информационно-телекоммуникационных технологий.
2. Назовите основные пути совершенствования механизмов взаимодействия правоохранительных и судебных органов разных стран по вопросам расследования киберпреступлений и судебного разбирательства по ним.

Вариант 14

1. Назовите основные вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
2. 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 вы можете назвать проблемы, возникающие при квалификации вовлечения несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов?

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 электронных средств платежа», указав его проблемные аспекты.

2. Дайте уголовно-правовую характеристику составу вовлечения несовершеннолетнего в совершение действий, представляющих опасность для его жизни, совершенное с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

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 кражи с банковского счета, а равно в отношении электронных денежных средств – в чем заключаются проблемы квалификации, каковы основные пути совершения такого деяния?

2. В чем заключаются основные вопросы квалификации мошенничества в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств)?

Вариант 22

1. Каковы основные проблемные аспекты квалификации незаконных организации и проведения азартных игр, совершаемых с использованием сети Интернет и иных информационно-телекоммуникационных сетей?

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

Примеры практических задач

Код формируемой компетенции (или ее части):

ПК-2.3, ПК-2.4, ПК-3.5.

Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика

Задача.

Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и окончательным оборудованием в смысле ст. 274 УК РФ? Какие виды окончательного оборудования возможны? Относится ли к окончательному оборудованию телефонный модем?

В качестве образца предлагается **решение задачи**:

В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.

Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона преступления характеризуется виной как в форме умысла, так и неосторожности.

Однако, вопрос об уголовной ответственности Шатурина зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Тема 2. Преступления в сфере компьютерной информации

Задача 1.

Инженер кафедры правовой информатики Т., нарушая правила эксплуатации ЭВМ, которые указаны в Инструкции по работе с ЭВМ, выключал компьютер, не закрывая текущих программ. Это привело к скоплению на жестком диске большого количества потерянных (недоступных) кластеров (участков памяти). К тому же, пренебрегая Инструкциями по эксплуатации ЭВМ, Т. не проводил регулярного технического обслуживания компьютера, что вызвало блокирование охраняемой законом информации, а также необходимость длительного ремонта компьютера.

Дайте уголовно-правовую оценку действиям Т.

Задача 2.

Работник НИИ М. разработал компьютерный вирус, поражающий текстовую информацию на компьютере, и продемонстрировал возможности этой программы коллеге Г., который без разрешения автора переписал программу-вирус на свою флэш-карту. Перед увольнением из НИИ Г., желая отомстить своему начальнику, инфицировал его компьютер этим вирусом, что повлекло изменение первоначальной информации на этом компьютере.

Квалифицируйте действия М. и Г. Имеются ли в их действиях признаки состава преступления?

Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий

Задача 1.

Жуликов, используя заранее приобретенное им программное обеспечение, и воспользовавшись доверием со стороны Потерпевшего, отправил последнему сообщение в Ватсапе в котором содержался файл «Архив.ар» и сообщение «Это ты на фотографии?». В результате открытия и автоматической установки файла «Архив.арк» Жуликов получил полный доступ к просмотру всей информации, которая демонстрируется на телефоне Потерпевшего.

Наблюдая за действиями потерпевшего, Жуликов получил данные о логине и пароле потерпевшего в систему «сбербанк онлайн». Далее Жуликов, на своем компьютере, воспользовавшись ранее полученной информацией, осуществил вход в систему сбербанк онлайн. Затем, используя программу, установленную на телефоне Потерпевшего, посмотрел коды, направленные Потерпевшему в СМС сообщениях с номера 900. Используя полученную информацию Жуликов, получил доступ в личный кабинет Потерпевшего и осуществил перевод денежных средств в размере 100 000 рублей на принадлежавший его сожительнице расчетный счет.

В момент осуществления действий сожительница Жуликова находилась рядом. Затем Жуликов попросил сожительницу сходить до банкомата и снять денежные средства, что она и сделала. Из снятых денежных средств

сожительница 80 000 рублей передала Жуликову, 10 000 рублей оставила себе в качестве вознаграждения (с позволения Жуликова), на 10 000 рублей приобрела спиртное и продукты питания, которые они совместно с Жуликовым употребили.

Квалифицируйте действия всех обозначенных лиц.

Задача 2.

Не позднее 29.01.2019 Воронов, руководствуясь корыстными побуждениями, обладая лидерскими и организаторскими способностями, будучи достоверно осведомленным о способе и особенностях совершения хищений денежных средств у граждан с использованием средств мобильной связи, с целью получения систематического незаконного материального дохода, решил создать на территории Республики Бурятия устойчивую организованную группу и руководить ею для совершения серии тяжких преступлений - хищений имущества, безналичных денежных средств, находящихся на банковских счетах граждан, открытых в Банке ВТБ (публичное акционерное общество)(далее по тексту Банк ВТБ (ПАО), Акционерном обществе "Альфа Банк" (далее по тексту АО "Альфа-банк", Акционерном обществе "Тинькофф Банк" (далее по тексту АО "Тинькофф Банк").

В совершенстве владея преступными навыками, имея познания в области использования информационных технологий (мобильных устройств с доступом в информационно-телекоммуникационную сеть Интернет), В. разработал план совершения хищений денежных средств с банковских счетов граждан, в соответствии с которым устойчивая организованная группа под его руководством должна была:

- располагая сведениями о владельцах сим-карт сотовых операторов и их персональных данных, а также о наличии банковских счетов, открытых в банках ВТБ (ПАО), АО "Альфа-банк", АО "Тинькофф Банк", зарегистрированных в системе "ВТБ-онлайн", мобильных приложениях "Альфа Мобайл", АО "Тинькофф Банк", выбрать граждан, являющихся клиентами вышеуказанных банков, у которых планировалось похитить денежные средства с банковских счетов;

- с использованием средства мобильной связи осуществить звонок на абонентский номер клиента Банка ВТБ (ПАО), АО "Альфа-банк", АО "Тинькофф Банк", и, представившись работником Банка, называя клиента по имени и отчеству, действуя с целью получения незаконного доступа к денежным средствам, находящимся на банковском счете, получить от клиента информацию о последних операциях по его банковской карте, после чего путем сообщения заведомо ложных сведений ввести гражданина в заблуждение относительно приостановления операций по банковской карте в результате попытки хищения денежных средств или в результате технического сбоя в работе банковской программы, либо иным способом, в дальнейшем использовать полученные сведения в целях хищения принадлежащих гражданину безналичных денежных средств, находящихся на счете банковской карты последнего;

- представляясь работником банка, предлагая услугу по отмене приостановления операций по банковской карте гражданина, убедить последнего сообщить реквизиты банковской карты, то есть сведения о номере банковской карты, сроке ее действия, а также данные о трехзначном коде безопасности (CVC/CVV), указанном на обратной стороне карты, который служит дополнительной защитой от несанкционированного списания денег со счета, в дальнейшем использовать полученные сведения в целях хищения принадлежащих гражданину безналичных денежных средств, находящихся на счете банковской карты последнего;

- используя мобильный телефон, оснащенный доступом к сети "Интернет", ввести полученные от гражданина вышеуказанные реквизиты банковской карты в электронной форме в мобильном приложении "ВТБ-онлайн", "Альфа Мобайл", АО "Тинькофф Банк" и перейти в графу "восстановление пароля";

- продолжая обманывать гражданина в ходе телефонного разговора, получить у последнего сведения о кодах и пароле, необходимых для восстановления пароля и для замены действующего пароля для получения доступа в онлайн-кабинет клиента в приложениях "ВТБ-онлайн", "Альфа Мобайл", АО "Тинькофф Банк", содержащиеся в последовательных sms-сообщениях, поступающих от банковских программ, обеспечивающих безопасность операций по банковским счетам клиентов без присутствия карты, на абонентский номер держателя банковской карты, и, таким образом, получить незаконный доступ к личному онлайн-кабинету гражданина в приложениях "ВТБ-онлайн", "Альфа Мобайл", АО "Тинькофф Банк", и, соответственно, к безналичным денежным средствам, находящимся на счете (счетах) банковской карты (карт) граждан и возможность несанкционированного перечисления их на находившиеся под контролем участников организованной группы банковские счета или карты либо электронных платежных систем ООО НКО "ЮМани" (до переименования 03.11.2020 - ООО НКО "Яндекс.Деньги") и VISA, оплату услуг операторов сотовой связи и совершении покупок на различных интернет-ресурсах;

- используя мобильный телефон, оснащенный доступом к сети "Интернет", полученные от гражданина коды и пароль, ввести в онлайн приложения, получив возможность совершения банковских операций в "личном кабинете" гражданина с безналичными денежными средствами, находящимися на счете, в целях их хищения.

В результате указанных преступных действий, при поступлении безналичных денежных средств гражданина или Банка на счет банковской карты либо электронного кошелька, находившихся под контролем участников организованной группы, распорядиться похищенным по своему усмотрению.

Реализуя указанную схему участники преступной группы совершили хищения денежных средств, принадлежащих более чем 10 гражданам.

Как правильно квалифицировать действия Воронова, с учетом, что все потерпевшие после ознакомления с смс-сообщениями о переводе денежных

средств с их банковских счетов добровольно сообщали одноразовые коды для проведения операций с денежными средствами.

Задача 3.

23.02.2025 Хитров, Быстров, Умнов и Наглов договорились о хищении денежных средств из предназначенных для их хранения и выдачи банкоматов Сбербанка. Реализуя задуманное, предварительно получив от неустановленного лица технические средства и программное обеспечение, необходимые для подключения к банкоматам, а также инструкции о порядке их применения для обеспечения выдачи банкоматами находящихся в них денежных средств, координируя с неустановленным лицом свои действия, в 02 часа 50 минут прибыли к офису Сбербанка.

Затем, из корыстных побуждений, с целью завладения чужим имуществом, убедившись, что за их действиями никто не наблюдает, взаимно дополняя действия друг друга, Умнов и Хитров остались в автомашине, припаркованной около данного операционного офиса, и стали следить за окружающей обстановкой с целью недопущения их обнаружения и задержания посторонними, а Быстров и Наглов прошли внутрь данного операционного офиса, где Наглов в указанном Быстровым месте на корпусе банкомата N, внутри которого хранились денежные средства в сумме 2 500 000 рублей, при помощи портативной газовой сварки прожег отверстие.

Не обнаружив за проделанным в корпусе данного банкомата отверстием разъемов, через которые Быстров мог подключить имевшиеся у них технические средства и использовать программное обеспечение для выдачи указанной суммы и, тем самым, не сумев завладеть указанными денежными средствами по независящим от них обстоятельствам, Быстров и Наглов покинули помещение операционного офиса и, продолжая совместные с Умновым и Хитровым преступные действия, проследовали к следующему помещению офиса Сбербанка.

После этого, около 03 часов 20 минут, взаимно дополняя действия друг друга, Умнов и Хитров оставшись в автомашине, припаркованной около офиса, продолжили следить за окружающей обстановкой с целью недопущения их обнаружения и задержания посторонними, а Быстров и Наглов прошли к банкомату, находящемуся внутри отделения Сбербанка, в котором хранились денежные средства в сумме 2 500 000 рублей, где Наглов в указанном Быстровым месте на корпусе банкомата, при помощи портативной газовой сварки вновь прожег отверстие. Однако подключиться к банкомату и осуществить выдачу денежных средств не успели по причине того, что были задержаны сотрудниками банка.

Однако, довести свой преступный умысел, направленный на хищение в составе группы лиц по предварительному сговору денежных средств, хранившихся в банкоматах Сбербанка, в результате которого ПАО «Сбербанк» мог быть причинен ущерб в особо крупном размере на общую сумму 5 000 000 рублей, указанные лица не смогли по независящим от них обстоятельствам, ввиду отсутствия технической возможности подключения через проделанное в

корпусе банкомата отверстие имевшегося у них оборудования для доступа к хранящимся в нем денежным средствам, а также пресечения их действий сотрудниками правоохранительных органов после прожигания отверстия в корпусе банкомата.

Квалифицируйте действия всех обозначенных лиц.

Тема 4. Проблемы квалификации киберпреступлений

Задача 1.

Жуликов, обладая познаниями в сфере ай-ти технологий создал программу, способную записывать отрывки разговоров и пересылать их на подконтрольный ему сервер. Преследуя корыстную цель, Жуликов создал ссылку, при переходе по которой скачивалось созданное им программное обеспечение.

Иванова Т.М. в поисках понравившейся ей песни, не осведомленная о содержании сайта, перешла по заранее подготовленной и замаскированной Жуликовым ссылке, скачала и установила вирус Жуликова.

В результате использования вируса Жуликов получил отрывки разговоров Ивановой Т.М. (по 2-3 слова, вырванные из контекста и не образующие смысловой нагрузки) и, используя чат искусственный интеллект, смог воссоздать речь Ивановой Т.М.

Затем Жуликов, используя программы, позволяющие подменить номер телефона, позвонил Иванову А.А. (супругу) с отображением номера телефона Ивановой Т.М. и ее голосом пояснил, что она сбила человека и срочно нужно перевести потерпевшему денежные средства в размере 300 000 рублей, иначе в отношении нее возбудят уголовное дело.

Опасаясь уголовного преследования, Иванов А.А. перевел на счет Маргиналова указанную сумму.

Далее Жуликов связался с Маргиналовым и пояснил в результате каких действий на счет Маргиналова поступили денежные средства, а также потребовал передать их Жуликову.

Маргиналов снял денежные средства со своей карты и в полном объеме передал их Жуликову. После этого Жуликов приобрел спиртное и продукты питания на общую сумму 2000 рублей и, в качестве благодарности, передал их Маргиналову.

Квалифицируйте действия всех обозначенных лиц.

Задача 2.

Б., старший научный сотрудник НИИ, был завербован иностранной разведкой для получения различного рода информации. В ходе предварительного расследования установлено, что Б. получил задание передать разведке содержащуюся в компьютере его коллеги информацию, которая является военной тайной, и, в качестве аванса, значительную сумму денег в иностранной валюте.

Столкнувшись в процессе переписывания информации с большими трудностями, по независящим от него обстоятельствам Б. не смог скопировать компьютерную информацию на другой магнитный носитель. Но ему удалось сфотографировать с экрана компьютера чертежи и прилагаемые к ним записи. При попытке передать фотопленку заказчику Б. был задержан работниками контрразведки.

Квалифицируйте действия Б.

Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе

Задача 1.

Сотрудник конструкторского бюро по разработке экспериментальных моделей двигателей для военных самолетов К. занимался системным обслуживанием компьютеров, но при этом он не обладал правом доступа к определенной группе файлов, защищенных паролем. По предложению агента конкурирующей иностранной фирмы К., за солидное вознаграждение, используя свои знания и навыки, узнал пароль доступа к секретной информации, которая хранилась в памяти ЭВМ. При очередном обслуживании компьютера, воспользовавшись удобным моментом, К. скопировал секретную информацию на переданный ему флэш-накопитель. Из-за разоблачения иностранного агента службой безопасности флэш-накопитель осталась невостребованным.

Имеются ли в действиях К. признаки состава преступления? Если «да», то дайте им уголовно-правовую оценку.

Задача 2.

Иностранный гражданин Ч., студент медицинского университета, поздно ночью проник в здание филиала коммерческого банка и похитил из сейфа различные документы, наличные деньги, а также несколько флэш-накопителей, предназначенных для работы с компьютером банка. Поскольку Ч. сам не разбирался в компьютерной технике, то он продал похищенные флэш-накопители своему знакомому К., который работал программистом в НИИ. Используя информацию, хранимую на флэш-накопителях, К. получил электронный доступ в банковский компьютер, в результате чего совершил хищение крупной суммы денег со счетов вкладчиков.

Решите вопрос об ответственности указанных в задаче лиц.

Критерии оценки решения практических задач:

Для оценивания решения задач используются следующие критерии: правильность по содержанию,

последовательность;
самостоятельность суждений и выводов;
степень развития логического мышления;
культура речи учащихся.

Каждый критерий оценивается в 1 балл, общая оценка складывается из суммы полученных баллов; максимальный балл за ответ – 5. Отказ от выполнения задания или отсутствие выполненного задания может быть оценено выставлением в журнал оценки «неудовлетворительно», влечет необходимость выполнения невыполненного задания и отработки соответствующей темы в форме, определяемой преподавателем.

6. Контрольно-измерительные материалы по дисциплине

Примерный перечень вопросов для подготовки к зачету

Код проверяемой компетенции (или ее части):

ПК-2.3.

1. Предмет, метод, задачи 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. Незаконное использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения.

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

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

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

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

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

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

17. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

18. Незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции.

19. Информация как предмет преступления.

20. Информационно-телекоммуникационные (кибернетические) технологии как способ и средство совершения преступления.

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

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

23. Преступления против жизни и здоровья, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

25. Преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

27. Преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

29. Преступления против общественной безопасности и общественного порядка, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

Код проверяемой компетенции (или ее части):
ПК-2.4.

31. Преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

32. Кража с банковского счёта или электронных денежных средств: проблемы квалификации, основные пути совершения.

33. Преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

35. Преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

36. Преступления против основ конституционного строя и безопасности государства, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

38. Преступления против мира и безопасности человечества, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

40. Преступления против государственной власти, интересов государственной службы, и службы местного самоуправления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

42. Преступления против половой свободы и половой

неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

44. Преступления против конституционных прав и свобод человека и гражданина, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

46. Преступления против порядка управления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

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

49. Нарушение неприкосновенности частной жизни, совершенное путем использования информационно-телекоммуникационных технологий.

50. 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 электронных средств платежа, 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, 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.

Код проверяемой компетенции (или ее части):

ПК-3.5.

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 использования 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.

77. Содействие диверсионной деятельности, прохождение обучения в целях осуществления диверсионной деятельности, организация диверсионного сообщества и участие в нем, осуществляемые с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

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

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

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

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

82. Соотношение неправомерного доступа к компьютерной информации и нарушения тайны переписки, телефонных переговоров, телеграфных и иных сообщений.

83. Подделка, изготовление или оборот поддельных цифровых документов, его соотношение со внесением несанкционированных изменений в государственные базы данных.

84. Нарушение неприкосновенности частной жизни, совершаемой путем неправомерного доступа к компьютерной информации.

85. Вопросы квалификации преступления, предусмотренного ст. 273 УК РФ: признак вредоносности программы и признак заведомости.

86. Определение момента окончания создания вредоносной компьютерной программы.

87. Проблемы определения малозначительности создания, распространения и использования вредоносных компьютерных программ.

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

89. Цифровые доказательства и их процессуальный статус.

90. Вопросы поддержания обвинения по делам о киберпреступлениях.

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

92. Конкуренция неправомерного доступа к компьютерной информации и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

93. Критическая информационная инфраструктура Российской Федерации как предмет преступления – отдельные проблемные аспекты определения.

94. Вопросы отграничения совокупности преступлений в сфере компьютерной информации от единого продолжаемого преступления.

95. Вопросы разграничения административных и уголовных дел в сфере связи и информации, а равно совершенных с использованием информационно-телекоммуникационных технологий.

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

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

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

Комплект задач для проведения экзамена

Код проверяемой компетенции (или ее части):

ПК-2.3.

Задача 1.

Инженер кафедры правовой информатики Т., нарушая правила эксплуатации ЭВМ, которые указаны в Инструкции по работе с ЭВМ, выключал компьютер, не закрывая текущих программ. Это привело к скоплению на жестком диске большого количества потерянных (недоступных) кластеров (участков памяти). К тому же, пренебрегая Инструкциями по эксплуатации ЭВМ, Т. не проводил регулярного технического обслуживания компьютера, что вызвало блокирование охраняемой законом информации, а также необходимость длительного ремонта компьютера.

Дайте уголовно-правовую оценку действиям Т.

Задача 2.

Работник НИИ М. разработал компьютерный вирус, поражающий текстовую информацию на компьютере, и продемонстрировал возможности этой программы коллеге Г., который без разрешения автора переписал программу-вирус на свою флэш-карту. Перед увольнением из НИИ Г., желая отомстить своему начальнику, инфицировал его компьютер этим вирусом, что повлекло изменение первоначальной информации на этом компьютере.

Квалифицируйте действия М. и Г. Имеются ли в их действиях признаки состава преступления?

Задача 3.

Жуликов, используя заранее приобретенное им программное обеспечение, и воспользовавшись доверием со стороны Потерпевшего, отправил последнему сообщение в Ватсапе в котором содержался файл «Архив.ар» и сообщение «Это ты на фотографии?». В результате открытия и автоматической установки файла «Архив.арк» Жуликов получил полный доступ к просмотру всей информации, которая демонстрируется на телефоне Потерпевшего.

Наблюдая за действиями потерпевшего, Жуликов получил данные о логине и пароле потерпевшего в систему «сбербанк онлайн». Далее Жуликов, на своем компьютере, воспользовавшись ранее полученной информацией, осуществил вход в систему сбербанк онлайн. Затем, используя программу, установленную на телефоне Потерпевшего, посмотрел коды, направленные Потерпевшему в СМС сообщениях с номера 900. Используя полученную информацию Жуликов, получил доступ в личный кабинет Потерпевшего и осуществил перевод денежных средств в размере 100 000 рублей на принадлежавший его сожительнице расчетный счет.

В момент осуществления действий сожительница Жуликова находилась рядом. Затем Жуликов попросил сожительницу сходить до банкомата и снять денежные средства, что она и сделала. Из снятых денежных средств

сожительница 80 000 рублей передала Жуликову, 10 000 рублей оставила себе в качестве вознаграждения (с позволения Жуликова), на 10 000 рублей приобрела спиртное и продукты питания, которые они совместно с Жуликовым употребили.

Квалифицируйте действия всех обозначенных лиц.

Задача 4.

Не позднее 29.01.2019 Воронов, руководствуясь корыстными побуждениями, обладая лидерскими и организаторскими способностями, будучи достоверно осведомленным о способе и особенностях совершения хищений денежных средств у граждан с использованием средств мобильной связи, с целью получения систематического незаконного материального дохода, решил создать на территории Республики Бурятия устойчивую организованную группу и руководить ею для совершения серии тяжких преступлений - хищений имущества, безналичных денежных средств, находящихся на банковских счетах граждан, открытых в Банке ВТБ (публичное акционерное общество)(далее по тексту Банк ВТБ (ПАО), Акционерном обществе "Альфа Банк" (далее по тексту АО "Альфа-банк", Акционерном обществе "Тинькофф Банк" (далее по тексту АО "Тинькофф Банк").

В совершенстве владея преступными навыками, имея познания в области использования информационных технологий (мобильных устройств с доступом в информационно-телекоммуникационную сеть Интернет), В. разработал план совершения хищений денежных средств с банковских счетов граждан, в соответствии с которым устойчивая организованная группа под его руководством должна была:

- располагая сведениями о владельцах сим-карт сотовых операторов и их персональных данных, а также о наличии банковских счетов, открытых в банках ВТБ (ПАО), АО "Альфа-банк", АО "Тинькофф Банк", зарегистрированных в системе "ВТБ-онлайн", мобильных приложениях "Альфа Мобайл", АО "Тинькофф Банк", выбрать граждан, являющихся клиентами вышеуказанных банков, у которых планировалось похитить денежные средства с банковских счетов;

- с использованием средства мобильной связи осуществить звонок на абонентский номер клиента Банка ВТБ (ПАО), АО "Альфа-банк", АО "Тинькофф Банк", и, представившись работником Банка, называя клиента по имени и отчеству, действуя с целью получения незаконного доступа к денежным средствам, находящимся на банковском счете, получить от клиента информацию о последних операциях по его банковской карте, после чего путем сообщения заведомо ложных сведений ввести гражданина в заблуждение относительно приостановления операций по банковской карте в результате попытки хищения денежных средств или в результате технического сбоя в работе банковской программы, либо иным способом, в дальнейшем использовать полученные сведения в целях хищения принадлежащих гражданину безналичных денежных средств, находящихся на счете банковской карты последнего;

- представляясь работником банка, предлагая услугу по отмене приостановления операций по банковской карте гражданина, убедить последнего сообщить реквизиты банковской карты, то есть сведения о номере банковской карты, сроке ее действия, а также данные о трехзначном коде безопасности (CVC/CVV), указанном на обратной стороне карты, который служит дополнительной защитой от несанкционированного списания денег со счета, в дальнейшем использовать полученные сведения в целях хищения принадлежащих гражданину безналичных денежных средств, находящихся на счете банковской карты последнего;

- используя мобильный телефон, оснащенный доступом к сети "Интернет", ввести полученные от гражданина вышеуказанные реквизиты банковской карты в электронной форме в мобильном приложении "ВТБ-онлайн", "Альфа Мобайл", АО "Тинькофф Банк" и перейти в графу "восстановление пароля";

- продолжая обманывать гражданина в ходе телефонного разговора, получить у последнего сведения о кодах и пароле, необходимых для восстановления пароля и для замены действующего пароля для получения доступа в онлайн-кабинет клиента в приложениях "ВТБ-онлайн", "Альфа Мобайл", АО "Тинькофф Банк", содержащиеся в последовательных sms-сообщениях, поступающих от банковских программ, обеспечивающих безопасность операций по банковским счетам клиентов без присутствия карты, на абонентский номер держателя банковской карты, и, таким образом, получить незаконный доступ к личному онлайн-кабинету гражданина в приложениях "ВТБ-онлайн", "Альфа Мобайл", АО "Тинькофф Банк", и, соответственно, к безналичным денежным средствам, находящимся на счете (счетах) банковской карты (карт) граждан и возможность несанкционированного перечисления их на находившиеся под контролем участников организованной группы банковские счета или карты либо электронных платежных систем ООО НКО "ЮМани" (до переименования 03.11.2020 - ООО НКО "Яндекс.Деньги") и VISA, оплату услуг операторов сотовой связи и совершении покупок на различных интернет-ресурсах;

- используя мобильный телефон, оснащенный доступом к сети "Интернет", полученные от гражданина коды и пароль, ввести в онлайн приложения, получив возможность совершения банковских операций в "личном кабинете" гражданина с безналичными денежными средствами, находящимися на счете, в целях их хищения.

В результате указанных преступных действий, при поступлении безналичных денежных средств гражданина или Банка на счет банковской карты либо электронного кошелька, находившихся под контролем участников организованной группы, распорядиться похищенным по своему усмотрению.

Реализуя указанную схему участники преступной группы совершили хищения денежных средств, принадлежащих более чем 10 гражданам.

Как правильно квалифицировать действия Воронова, с учетом, что все потерпевшие после ознакомления с смс-сообщениями о переводе денежных

средств с их банковских счетов добровольно сообщали одноразовые коды для проведения операций с денежными средствами.

Код проверяемой компетенции (или ее части):
ПК-2.4.

Задача 5.

23.02.2025 Хитров, Быстров, Умнов и Наглов договорились о хищении денежных средств из предназначенных для их хранения и выдачи банкоматов Сбербанка. Реализуя задуманное, предварительно получив от неустановленного лица технические средства и программное обеспечение, необходимые для подключения к банкоматам, а также инструкции о порядке их применения для обеспечения выдачи банкоматами находящихся в них денежных средств, координируя с неустановленным лицом свои действия, в 02 часа 50 минут прибыли к офису Сбербанка.

Затем, из корыстных побуждений, с целью завладения чужим имуществом, убедившись, что за их действиями никто не наблюдает, взаимно дополняя действия друг друга, Умнов и Хитров остались в автомашине, припаркованной около данного операционного офиса, и стали следить за окружающей обстановкой с целью недопущения их обнаружения и задержания посторонними, а Быстров и Наглов прошли внутрь данного операционного офиса, где Наглов в указанном Быстровым месте на корпусе банкомата N, внутри которого хранились денежные средства в сумме 2 500 000 рублей, при помощи портативной газовой сварки прожег отверстие.

Не обнаружив за проделанным в корпусе данного банкомата отверстием разъемов, через которые Быстров мог подключить имевшиеся у них технические средства и использовать программное обеспечение для выдачи указанной суммы и, тем самым, не сумев завладеть указанными денежными средствами по независящим от них обстоятельствам, Быстров и Наглов покинули помещение операционного офиса и, продолжая совместные с Умновым и Хитровым преступные действия, проследовали к следующему помещению офиса Сбербанка.

После этого, около 03 часов 20 минут, взаимно дополняя действия друг друга, Умнов и Хитров оставшись в автомашине, припаркованной около офиса, продолжили следить за окружающей обстановкой с целью недопущения их обнаружения и задержания посторонними, а Быстров и Наглов прошли к банкомату, находящемуся внутри отделения Сбербанка, в котором хранились денежные средства в сумме 2 500 000 рублей, где Наглов в указанном Быстровым месте на корпусе банкомата, при помощи портативной газовой сварки вновь прожег отверстие. Однако подключиться к банкомату и осуществить выдачу денежных средств не успели по причине того, что были задержаны сотрудниками банка.

Однако, довести свой преступный умысел, направленный на хищение в составе группы лиц по предварительному сговору денежных средств, хранившихся в банкоматах Сбербанка, в результате которого ПАО «Сбербанк»

мог быть причинен ущерб в особо крупном размере на общую сумму 5 000 000 рублей, указанные лица не смогли по независящим от них обстоятельствам, ввиду отсутствия технической возможности подключения через проделанное в корпусе банкомата отверстие имевшегося у них оборудования для доступа к хранящимся в нем денежным средствам, а также пресечения их действий сотрудниками правоохранительных органов после прожигания отверстия в корпусе банкомата.

Квалифицируйте действия всех обозначенных лиц.

Задача 6.

Жуликов, обладая познаниями в сфере ай-ти технологий создал программу, способную записывать отрывки разговоров и пересылать их на подконтрольный ему сервер. Преследуя корыстную цель, Жуликов создал ссылку, при переходе по которой скачивалось созданное им программное обеспечение.

Иванова Т.М. в поисках понравившейся ей песни, не осведомленная о содержании сайта, перешла по заранее подготовленной и замаскированной Жуликовым ссылке, скачала и установила вирус Жуликова.

В результате использования вируса Жуликов получил отрывки разговоров Ивановой Т.М. (по 2-3 слова, вырванные из контекста и не образующие смысловой нагрузки) и, используя чат искусственный интеллект, смог воссоздать речь Ивановой Т.М.

Затем Жуликов, используя программы, позволяющие подменить номер телефона, позвонил Иванову А.А. (супругу) с отображением номера телефона Ивановой Т.М. и ее голосом пояснил, что она сбита человека и срочно нужно перевести потерпевшему денежные средства в размере 300 000 рублей, иначе в отношении нее возбудят уголовное дело.

Опасаясь уголовного преследования, Иванов А.А. перевел на счет Маргиналова указанную сумму.

Далее Жуликов связался с Маргиналовым и пояснил в результате каких действий на счет Маргиналова поступили денежные средства, а также потребовал передать их Жуликову.

Маргиналов снял денежные средства со своей карты и в полном объеме передал их Жуликову. После этого Жуликов приобрел спиртное и продукты питания на общую сумму 2000 рублей и, в качестве благодарности, передал их Маргиналову.

Квалифицируйте действия всех обозначенных лиц.

Задача 7.

Б., старший научный сотрудник НИИ, был завербован иностранной разведкой для получения различного рода информации. В ходе предварительного расследования установлено, что Б. получил задание передать разведке содержащуюся в компьютере его коллеги информацию, которая

является военной тайной, и, в качестве аванса, значительную сумму денег в иностранной валюте.

Столкнувшись в процессе переписывания информации с большими трудностями, по независящим от него обстоятельствам Б. не смог скопировать компьютерную информацию на другой магнитный носитель. Но ему удалось сфотографировать с экрана компьютера чертежи и прилагаемые к ним записи. При попытке передать фотопленку заказчику Б. был задержан работниками контрразведки.

Квалифицируйте действия Б.

Код проверяемой компетенции (или ее части):

ПК-3.5.

Задача 8.

Сотрудник конструкторского бюро по разработке экспериментальных моделей двигателей для военных самолетов К. занимался системным обслуживанием компьютеров, но при этом он не обладал правом доступа к определенной группе файлов, защищенных паролем. По предложению агента конкурирующей иностранной фирмы К., за солидное вознаграждение, используя свои знания и навыки, узнал пароль доступа к секретной информации, которая хранилась в памяти ЭВМ. При очередном обслуживании компьютера, воспользовавшись удобным моментом, К. скопировал секретную информацию на переданный ему флэш-накопитель. Из-за разоблачения иностранного агента службой безопасности флэш-накопитель остался невостребованным.

Имеются ли в действиях К. признаки состава преступления? Если «да», то дайте им уголовно-правовую оценку.

Задача 9.

Иностранный гражданин Ч., студент медицинского университета, поздно ночью проник в здание филиала коммерческого банка и похитил из сейфа различные документы, наличные деньги, а также несколько флэш-накопителей, предназначенных для работы с компьютером банка. Поскольку Ч. сам не разбирался в компьютерной технике, то он продал похищенные флэш-накопители своему знакомому К., который работал программистом в НИИ. Используя информацию, хранимую на флэш-накопителях, К. получил электронный доступ в банковский компьютер, в результате чего совершил хищение крупной суммы денег со счетов вкладчиков.

Решите вопрос об ответственности указанных в задаче лиц.

Задача 10.

Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать

на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и окончательным оборудованием в смысле ст. 274 УК РФ? Какие виды окончательного оборудования возможны? Относится ли к окончательному оборудованию телефонный модем?

Образец билета к зачету

Билет № 1

1. Современное состояние киберпреступности, ее уровень, структура и динамика
2. Неправомерный доступ к охраняемой законом компьютерной информации
3. Задача.

Студент физико-математического факультета университета О., занимаясь самостоятельной работой на компьютере, создал вирусную программу, которая могла бы привести к порче монитора ЭВМ. Данной программой он «заразил» компьютерную игру, дискету с которой передал своему другу И. для установки на его компьютер. Через некоторое время И., решив в очередной раз запустить игру на выполнение, обнаружил, что изображение на экране компьютера исчезло. Позже выяснилось, что по причине инфицирования компьютера вирусом монитор вышел из строя.

Дайте юридическую оценку действиям О.

Шкала и критерии оценивания на зачете

Оценка «зачтено» выставляется, если студент ответил на теоретические вопросы, содержащиеся в билете, правильно решил задачу продемонстрировав:

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках информационно-телекоммуникационных технологий 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 информационно-

телекоммуникационными технологиями 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 информационно-телекоммуникационных технологий, 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 теоретические вопросы, содержащиеся в билете, либо допустил грубые ошибки при ответе на теоретические вопросы, показав тем самым отсутствие вышеперечисленных знаний, умений, навыков.