

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

Дальневосточный юридический институт (филиал)

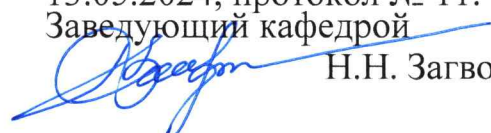
Кафедра уголовно-правовых дисциплин

УТВЕРЖДЕН

на совместном заседании кафедр

13.05.2024, протокол № 11.

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 – 2024

Очная форма обучения

Владивосток, 2024

Фонд оценочных средств по учебной дисциплине «Противодействие киберпреступности» обсужден и одобрен на совместном заседании кафедр Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации 13.05.2024, протокол № 11.

Авторы-составители:

Винокуров Максим Владимирович	Доцент кафедры уголовно-правовых дисциплин Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации
Гундерич Альбина Альбертовна	Доцент кафедры уголовно-правовых дисциплин Крымского юридического института (филиала) Университета прокуратуры Российской Федерации, к.ю.н., доцент
Лобач Дмитрий Владимирович	Доцент кафедры теории и истории государства и права Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, к.ю.н.
Побегайло Анастасия Эдуардовна	доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации кандидат юридических наук
Попов Александр Николаевич	заведующий кафедрой уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, д.ю.н., профессор
Тихонов Александр Николаевич	Заведующий отделом Луганского юридического института (филиала) Университета прокуратуры Российской Федерации, к.ю.н., доцент

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.

© Университет прокуратуры
Российской Федерации, 2023.
© Винокуров М.В., Гундерич А. А.,
Лобач Д.В., Побегайло А.Э.,
Попов А.Н., Тихонов А.Н. 2024,

Цель фонда оценочных средств

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся по учебной дисциплине «Квалификация преступлений против личности». 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»».

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

Код компетенции	Содержание компетенции	Этап формирования	Предшествующий этап (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	7	6 этап - гражданское право, гражданский процесс, финансовое право, прокурорский надзор, 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.

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).

Паспорт фонда оценочных средств по дисциплине «Квалификация преступлений против личности»

<i>№ п/п</i>	<i>Наименование оценочных материалов</i>	<i>Виды контроля</i>	<i>Код контролируемой компетенции (код индикатора компетенции)</i>
1.	Вопросы для подготовки к зачету	Промежуточная аттестация	ПК-2 (ПК-2.3)
2.	Аудиторная контрольная работа	Текущий контроль	ПК-2 (ПК-2.3)
3.	Практическая письменная работа	Текущий контроль	ПК-2 (ПК-2.3)

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

Обучающийся знает: основные нормативные правовые акты, регламентирующие деятельность, направленную на защиту общественных отношений в сфере защиты прав, свобод, законных интересов человека и гражданина; положения Пленума Верховного Суда РФ по вопросам применения норм уголовного законодательства, направленных на защиту общественных отношений в сфере защиты прав, свобод, законных интересов человека и гражданина.

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. 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. 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.

17. Информация как предмет преступления.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

40. Преступления против половой свободы и половой неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

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

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

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

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

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

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

48. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенные с использованием киберсредств.

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

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

51. Мошенничество, совершенное с использованием электронных средств платежа, осуществляемое с применением кибертехнологий.

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

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

54. Кибертерроризм – определение, предмет и способы совершения.

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

56. 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.

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

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

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

60. Развратные действия, совершаемые путем использования ресурсов

сети Интернет.

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

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

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

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

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

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

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

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

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

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

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

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

73. 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.

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

75. 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).

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

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

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

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

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

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

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

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

84. Определение момента окончания создания вредоносной компьютерной программы.

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

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

87. Цифровые доказательства и их процессуальный статус.

88. Вопросы поддержания обвинения по делам о киберпреступлениях.

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

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

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

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

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

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

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

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

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

Обучающийся умеет: анализировать нормы действующего уголовного законодательства РФ, направленные на противодействие киберпреступности, положения Пленума Верховного Суда РФ по соответствующим вопросам; на основе проведенного анализа делать правильные выводы, квалифицировать факты и общественные отношения.

Обучающийся владеет: навыками анализа основных нормативных правовых актов, регламентирующих деятельность, направленную на противодействие киберпреступности, положений Пленума Верховного Суда РФ по соответствующим вопросам; навыками квалификации фактов и общественных отношений.

Задача

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.

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 *«отлично»* выставляется, если студент ответил на теоретические вопросы, содержащиеся в билете, решил практическое задание без ошибок; глубоко и прочно усвоил программный материал; исчерпывающе, грамотно и логически стройно излагает ответы на поставленные вопросы. При этом студент демонстрирует высокий уровень:

- знаний: уголовного законодательства и практики его применения; постановлений Пленума Верховного Суда Российской Федерации по уголовным делам; принципов, общих и частных правил квалификации киберпреступлений;

- умений: осуществлять уголовно-правовую оценку преступлений в точном соответствии с уголовным и уголовно-процессуальным законодательством, принципами и правилами квалификации преступлений; применять уголовно-правовые нормы во взаимосвязи с предписаниями иных отраслей права для квалификации киберпреступлений; проверять правильность их квалификации, выявлять ошибки, допущенные при квалификации киберпреступлений; грамотно мотивировать и оформить результаты квалификации киберпреступлений;

- навыков: анализа фактических обстоятельств совершения киберпреступления, выявления среди них тех фактов и обстоятельств, которые имеют уголовно-правовое значение; правильной уголовно-правовой оценки преступлений, выявления квалификационных ошибок; мотивировки решений о квалификации преступлений и ее отражения в процессуальных документах.

Оценка «хорошо» выставляется, если студент ответил на теоретические вопросы, содержащиеся в билете, допустив незначительные неточности, решил практическое задание без существенных ошибок, продемонстрировав:

- *знания*: уголовного законодательства и практики его применения; постановлений Пленума Верховного Суда Российской Федерации по уголовным делам; принципов, общих и частных правил квалификации киберпреступлений;

- *умения*: осуществлять уголовно-правовую оценку киберпреступлений в точном соответствии с уголовным и уголовно-процессуальным законодательством, принципами и правилами квалификации киберпреступлений; применять уголовно-правовые нормы во взаимосвязи с предписаниями иных отраслей права для квалификации киберпреступлений; проверять правильность их квалификации, выявлять ошибки, допущенные при квалификации киберпреступлений; грамотно мотивировать и оформить результаты квалификации киберпреступлений;

- *навыки*: анализа фактических обстоятельств совершения киберпреступления, выявления среди них тех фактов и обстоятельств, которые имеют уголовно-правовое значение; правильной уголовно-правовой оценки киберпреступлений, выявления квалификационных ошибок; мотивировки решений о квалификации киберпреступлений и ее отражения в процессуальных документах.

Оценка «удовлетворительно» выставляется, если студент с ошибками ответил на теоретические вопросы, содержащиеся в билете, решил практическое задание без грубых ошибок, продемонстрировав базовые:

- *знания*: уголовного законодательства и практики его применения; постановлений Пленума Верховного Суда Российской Федерации по уголовным делам; принципов, общих и частных правил киберквалификации преступлений;

- *умения*: осуществлять уголовно-правовую оценку киберпреступлений в точном соответствии с уголовным и уголовно-процессуальным законодательством, принципами и правилами квалификации киберпреступлений; применять уголовно-правовые нормы во взаимосвязи с предписаниями иных отраслей права для квалификации киберпреступлений; проверять правильность их квалификации, выявлять ошибки, допущенные при квалификации киберпреступлений; грамотно мотивировать и оформить результаты квалификации киберпреступлений;

- *навыки*: анализа фактических обстоятельств совершения киберпреступления, выявления среди них тех фактов и обстоятельств, которые имеют уголовно-правовое значение; правильной уголовно-правовой оценки киберпреступлений, выявления квалификационных ошибок; мотивировки решений о квалификации преступлений и ее отражения в процессуальных документах.

Оценка «неудовлетворительно» выставляется, если студент не ответил на теоретические вопросы, содержащиеся в билете, не решил практическое задание либо допустил грубые ошибки при ответе на теоретические вопросы и

при решении практического задания, показав тем самым отсутствие вышеперечисленных знаний, умений, навыков.

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

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).

Практическая письменная работа по дисциплине «Противодействие киберпреступности»

(Типовая)

Вариант 1

Задача. 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.

Вариант 2

Задача. 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.

Шкала и критерии оценивания практической письменной работы

- правильность решения задач;
- полнота решения задач;
- изложение нескольких теоретических подходов к освещаемой проблеме;

- полнота, последовательность, обоснованность изложенной позиции, в том числе подтвержденная ссылкой на правовые позиции высших судов, иную судебную практику.

Оценка *«отлично»* выставляется, если студент правильно и полно решил все задачи, обосновав свое решение со ссылкой на законодательство, правовые позиции высших судов, иную судебную практику, теоретические источники.

Оценка *«хорошо»* выставляется, если студент правильно и полно решил не все задачи, обосновав свое решение со ссылкой на законодательство, правовые позиции высших судов, иную судебную практику, теоретические источники, и правильно решив задачи, не обосновал в полной мере свое решение.

Оценка *«удовлетворительно»* выставляется в следующих случаях:

- студент правильно решил задачи, не обосновав свое решение;

- правильно и полно решил одну задачу, обосновав свое решение со ссылкой на законодательство, правовые позиции высших судов, иную судебную практику, теоретические источники, и неправильно решил другие задачи.

Оценка *«неудовлетворительно»* выставляется, если студент неправильно решил все задачи.