МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
уголовного права
(наименование ф-та полностью)

_____А.А. Байбарин
(подпись, инициалы, фамилия)

«27» июня 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине

Преступность в сфере высоких технологий
(наименование дисциплины)

ОПОП ВО 40.05.02 Правоохранительная деятельность
шифр и наименование направления подготовки (специальности)

специализация «Воспитательно-правовая»
наименование направленности (профиля, специализации)

Курск – 2022

1 Оценочные средства для текущего контроля успеваемости

1.1 Вопросы для устного опроса

1. Понятие и общая характеристика преступлений в сфере высоких технологий

1. Чем обусловлена актуальность изучения преступности в сфере высоких технологий в современный период?
2. Какие виды преступности относятся к высокотехнологичным?
3. Каково состояние киберпреступности и перспективы борьбы с ней?
4. В чём отличие распространённых представлений о личности киберпреступников от реальной действительности?
5. Чем обусловлено вовлечение в киберпреступность всё большего числа граждан?
6. Какие основные акты в сфере борьбы с преступностью технологий были приняты мировым сообществом?
7. Применяются ли эти акты в России?
8. Какие акты национального законодательства содержат нормы, направленные на борьбу с киберпреступностью?

2. Компьютерная информация как объект уголовно-правовой охраны

9. Каковы основные признаки информации?
10. В чём отличие информации от материи и энергии?
11. Каковы основные признаки компьютерной информации?
12. Что такое архитектура фон Неймана?
13. Какие права, связанные с информацией, закрепляются в Конституции РФ?
14. Какие права имеет обладатель информации?
15. Какие обязанности имеет обладатель информации?
16. Что такое «конфиденциальность информации»?
17. Какими видами мер обеспечивается информационная безопасность?
18. Каков родовой и видовой объект компьютерных преступлений?

3. Неправомерный доступ к компьютерной информации

19. Каковы основные признаки компьютерной информации?
20. В каком случае доступ к информации будет считаться неправомерным?
21. Является ли удаление файла в компьютере удалением информации?
22. В чём отличие модификации и уничтожения информации?
23. Происходит ли копирование информации при ознакомлении с ней?
24. Что такое крупный ущерб и тяжкие последствия в контексте ст. 272 УК РФ?
25. Что подразумевается под использованием служебного положения?
26. Каковы основные способы неправомерного доступа к информации?

4. Создание, использование и распространение вредоносных компьютерных программ

27. Чем вредоносная программа отличается от обычной?
28. Как следует оценивать создание программ, которые могут использоваться как в полезных, так и во вредоносных целях?
29. Какие основные типы вредоносных программ распространены в настоящее время?
30. Может ли быть привлечён к ответственности программист, ошибочно включивший в программу функции, которые могут привести к потере данных пользователя?
31. Какие обстоятельства влияют на размер ответственности по данной статье?
32. Как следует расценивать разработку и распространение программ, позволяющих осуществлять незаконное копирование объектов авторского права?

5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

33. Какие нормативные акты предусматривают специальные правила безопасной эксплуатации компьютерной техники и информационных сетей?
34. Охватываются ли составом данного преступления атаки типа «отказ в обслуживании» (DoS)?
35. Охватывается ли составом данного преступления неустановка системным администратором антивируса на компьютеры предприятия?
36. Кто является субъектом данного преступления?
37. Какова форма вины в данном преступлении?
38. Может ли наступать уголовная ответственность по данной статье за нарушение условий лицензионного договора?

6. Посягательства на авторские и смежные права в компьютерных сетях

39. Все ли программы могут рассматриваться как объект авторских прав?
40. Какие действия с программой пользователь может осуществлять без согласия автора?
41. Какие технические средства можно использовать для защиты авторских прав?
42. Что такое пиринговые сети?
43. Каков размер нарушенных прав, необходимый для привлечения лица к уголовной ответственности?

7. Хищения с использованием новых информационных технологий

44. Как квалифицируется получение в банкомате денег по чужой платёжной карте?
45. Совершение каких видов хищений возможно с использованием компьютерной техники?
46. Как квалифицируются многоэпизодные хищения?
47. Как квалифицируется использование вредоносных программ для совершения хищения?
48. Возможна ли квалификация хищений по совокупности с преступлениями в сфере компьютерной информации?

8. Распространение порнографии в компьютерных сетях

49. Что такое порнография? Есть ли законодательное определение данного понятия?
50. Какие виды порнографии различаются законодателем?
51. Существуют ли законные способы распространения порнографии?
52. Возможна ли борьба с порнографией в условиях существования глобальных компьютерных сетей?

Шкала оценивания: 5-балльная.

Критерии оценивания:

5 баллов (или оценка «отлично») выставляется обучающемуся, если задача решена правильно, в установленное преподавателем время или с опережением времени, при этом обучающимся предложено оригинальное (нестандартное) решение, или наиболее эффективное решение, или наиболее рациональное решение, или оптимальное решение.

4 балла (или оценка «хорошо») выставляется обучающемуся, если задача решена правильно, в установленное преподавателем время, типовым способом; допускается наличие несущественных недочетов.

3 балла (или оценка «удовлетворительно») выставляется обучающемуся, если при решении задачи допущены ошибки некритического характера и (или) превышено установленное преподавателем время.

2 балла (или оценка «неудовлетворительно») выставляется обучающемуся, если задача не решена или при ее решении допущены грубые ошибки.

1.2 Темы рефератов

1. Понятие и общая характеристика преступлений в сфере высоких технологий

1. Социально-культурологический портрет «хакера»
2. Международно-правовое регулирование борьбы с киберпреступностью
3. История российского законодательства о борьбе с киберпреступностью

2. Компьютерная информация как объект уголовно-правовой охраны

4. История российского законодательства об информационном обороте и информационной безопасности
5. Доктрина информационной безопасности РФ
6. Основные стандарты обеспечения информационной безопасности

3. Неправомерный доступ к компьютерной информации

7. Основные методы защиты от неправомерного доступа
8. Личность преступника, совершающего неправомерный доступ к компьютерной информации.
9. Понятие «компьютерная информация»

4. Создание, использование и распространение вредоносных компьютерных программ

10. История вредоносных программ.
11. Ботнеты.
12. Вредоносные программы как средство информационной войны.

5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

13. DDoS-атаки и уголовно-правовое противодействие им
14. Основные правила эксплуатации компьютерной техники
15. Основные правила эксплуатации средств хранения данных
16. Основные правила эксплуатации компьютерных сетей

6. Посягательства на авторские и смежные права в компьютерных сетях

17. Технические средства защиты авторского права и ответственность за их обход
18. Уголовная ответственность за нарушения авторского права с использованием пиринговых сетей
19. Методики оценки ущерба от нарушений авторских прав в компьютерных сетях.

7. Хищения с использованием новых информационных технологий

20. Хищения с использованием банковских платёжных карт
21. История использования компьютеров для совершения хищений
22. Компьютерное вымогательство

8. Распространение порнографии в компьютерных сетях

23. Определение понятия «порнография»
24. Методы борьбы с распространением порнографии в Интернете
25. Законодательство стран мира о порнографии

Шкала оценивания: 5-балльная.
Критерии оценивания:

5 баллов (или оценка «отлично») выставляется обучающемуся, если тема реферата раскрыта полно и глубоко, при этом убедительно и аргументированно изложена собственная позиция автора по рассматриваемому вопросу; структура реферата логична; изучено большое количество актуальных источников, грамотно сделаны ссылки на источники; самостоятельно подобран яркий иллюстративный материал; сделан обоснованный убедительный вывод; отсутствуют замечания по оформлению реферата.

4 балла (или оценка «хорошо») выставляется обучающемуся, если тема реферата раскрыта полно и глубоко, сделана попытка самостоятельного осмысления темы; структура реферата логична; изучено достаточное количество источников, имеются ссылки на источники; приведены уместные примеры; сделан обоснованный вывод; имеют место незначительные недочеты в содержании и (или) оформлении реферата.

3 балла (или оценка «удовлетворительно») выставляется обучающемуся, если тема реферата раскрыта неполно и (или) в изложении темы имеются недочеты и ошибки; структура реферата логична; количество изученных источников менее рекомендуемого, сделаны ссылки на источники; приведены общие примеры; вывод сделан, но имеет признаки неполноты и неточности; имеются замечания к содержанию и (или) оформлению реферата.

2 балла (или оценка «неудовлетворительно») выставляется обучающемуся, если содержание реферата имеет явные признаки плагиата и (или) тема реферата не раскрыта и (или) в изложении темы имеются грубые ошибки; материал не структурирован, излагается непоследовательно и сбивчиво; количество изученных источников значительно менее рекомендуемого, неправильно сделаны ссылки на источники или они отсутствуют; не приведены примеры или приведены неверные примеры; отсутствует вывод или вывод расплывчат и неконкретен; оформление реферата не соответствует требованиям.

1.3 Кейс-задачи

Неправомерный доступ к компьютерной информации

1. Сотрудники отдела «К» УВД г. Энска А. и З. для повышения показателей раскрываемости компьютерных преступлений решили провести «оперативный эксперимент». Найдя в газете бесплатных объявлений объявление об оказании услуг «компьютерной помощи», они позвонили давшему его Р. и попросили его оказать помощь в установке на компьютер программного продукта Autodesk Alias Surface 2016 (стоимость лицензии на который составляла 1 млн. 145 тыс. рублей). Поначалу Р. отказался, однако после повторных звонков и обещания дополнительного вознаграждения всё же согласился. Требуемую программу он скачал из Интернета, там же он нашёл средства, позволяющие обойти технические ограничения, связанные с защитой авторских прав. Для установки программы был подготовлен компьютер, содержащий «чистую» ОС Windows. После того, как Р. закончил установку и «взломал» программу, оперативники задержали его. Р. было предъявлено обвинение в покушении на совершение нарушения авторских и смежных прав в особо крупном размере, неправомерный доступ к компьютерной информации, совершённый из корыстной заинтересованности и причинивший крупный ущерб, а также в использовании вредоносных компьютерных программ, предназначенных для нейтрализации средств защиты компьютерной информации, совершённое из корыстной заинтересованности и причинивший крупный ущерб. Правильна ли такая квалификация? Правомерны ли действия оперативников?
2. В период с июня по декабрь 2012 г. руководитель малого предприятия Паршин совместно с кассиром Кондратьевой, действуя с единым умыслом, направленным на сокрытие доходов от налогообложения, ежедневно с 17 до 19 ч в торговых палатках предприятия подключали в гнезда двух контрольно-кассовых аппаратов специально изготовленный самодельный прибор, уничтожали информацию о проведен-

ных в течение текущей смены финансовых операциях и вносили измененные данные о сумме выручки.

Создание, использование и распространение вредоносных компьютерных программ

3. К., обнаружив в интернете сайт, на котором представители кавказских национальностей обсуждали способы знакомства с русскими девушками, движимый мотивом неприязни к лицам указанных национальностей, разместил на одном из популярных интернет-форумов своё описание ситуации, в котором в грубой форме с использованием матерной брани высказал мнение о неполноценности лиц указанных национальностей. К сообщению К. приложил ссылку на программу «Low Orbit Ion Cannon», предназначенную для организации интернет-атак типа «распределённый отказ в обслуживании» (DDoS) и инструкцию по её использованию для приведения в неработоспособное состояние указанного им сайта. Согласно записям в техническом журнале форума, программу скачали 2530 человек. В ходе следственных мероприятий была установлена личность 120 из них, доказать факт использования программы удалось в отношении 10. В результате атаки сайт не работал две недели, в результате перегрузки оборудования владельцу оборудования ООО «Самшит», на котором размещался сайт, был причинён ущерб 30 тысяч рублей, на восстановление сайта и перенос его на другой сервер его владельцем Г. было потрачено 50 тысяч рублей. Кроме того, Ч., один из пользователей форума, на котором К. разместил сообщение, подобрав пароль администратора сайта, скопировал личные данные 1300 пользователей сайта (электронные адреса, пароли, анкеты для знакомств) и разместил их на том же форуме. Дайте полную юридическую оценку деяния.
4. Боровиков, являясь оператором ЭВМ в одной из организаций, на своем компьютере изготовил электронное почтовое сообщение с рекламой товаров, приложив к нему в качестве подробного каталога с ценами составленную им программу ЭВМ, и распространил ее в сети Интернет 350 адресатам. В результате массового распространения этой программы после ее запуска пользователями сети Интернет, Боровиков несанкционированно получил по своему электронному адресу 87 учетных имен и паролей для доступа в Интернет, которые скопировал на жесткий диск своего компьютера и в дальнейшем использовал для доступа в сеть Интернет.
5. Специалисту по ЭВМ Коновалову была поручена разработка программы поиска необходимой информации. После ее установки была блокирована локальная сеть ЭВМ организации и частично уничтожена информация, вследствие того что новая программа содержала «троянского коня». Коновалов заявил, что он сделал это специально, потому что хотел отомстить директору организации за то, что тот встречался с его женой. Организация потерпела огромные убытки, так как пришлось восстанавливать информацию, которую накапливали годами.
6. АО «Окно» разработало и продавало компьютерную игру. При установке игры на компьютер некоторые стандартные драйверы устройств заменялись на драйверы, разработанные АО «Окно», в результате была нарушена нормальная работа нескольких тысяч компьютеров. При установке программа тестировала компьютерное оборудование и программное обеспечение пользователя, сведения о которых при регистрации с помощью модема сообщались в АО «Окно». В документации к игре не сообщалось об этом. Квалифицируйте содеянное.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

7. На сборочном конвейере Волжского автомобильного завода программист из мести руководству организации внес изменения в программу ЭВМ, управляющей подачей деталей на конвейер. В результате сбоя работы конвейера, который останавли-

вался при подаче на него определенного числа деталей, заводу был причинен ущерб в виде 200 невыпущенных автомобилей в смену.

8. Индивидуальный предприниматель Гончаров из корыстных побуждений отключил в рабочее время в офисе своего конкурента Борисова электричество, что привело к уничтожению деловой информации, обрабатываемой в это время в сети ЭВМ фирмы, и причинило Борисову значительный материальный ущерб.
9. 14-летний Сонин провел в компьютерном клубе 12 часов. Когда он пришел домой, ему стало плохо. Вызвали скорую помощь, отвезли его в больницу, где он провел в реанимации семь дней. Усилия врачей оказались тщетны — ребенок умер. Установленная причина смерти — острое нарушение мозгового кровообращения — инсульт. По мнению врачей, у Сонина произошла декомпенсаторная реакция на фоне переутомления, а мерцание компьютерного экрана в темной комнате спровоцировало именно такую реакцию головного мозга. Есть ли основания для привлечения к ответственности владельцев компьютерного клуба? Должны ли нести уголовную ответственность родители мальчика?

Хищения с использованием новых информационных технологий

10. Сотрудники вычислительного центра банка «Уникум» Каталов, Арбузов и Григорьев, имея доступ к компьютерной программе учета, ведения и оформления банковских операций отдела текущих счетов, изменили ее таким образом, что она позволяла округлять размеры платежей, а разницу перечислять на счет, открытый женой Каталова. Затем жена Каталова сняла со счета деньги в размере 120 тыс. руб., которые Каталов, Арбузов и Григорьев поделили поровну.
11. Группа из восьми лиц в возрасте от 20 до 36 лет, возглавляемая Лупиносом, осуществляла несанкционированный доступ к сайтам ряда коммерческих банков, получая таким образом информацию о клиентах этих финансовых учреждений. По электронной почте пострадавшим направлялись письма якобы от известных компаний. В письмах прятался вирус-троян. Он преодолевал защиту компьютера и открывал доступ к информации. В итоге таких электронных атак указанные лица переводили на свои счета крупные суммы денег, уничтожая при этом всю базу данных на компьютерах владельцев. Как квалифицировать действия группы лиц, возглавляемой Лупиносом?
12. 22-летний Виртальский специализировался на создании хакерских программ. Он не только создавал бот-системы и массово распространял вредоносные программы, но и лично принимал участие в хищении денег с различных счетов. Мишенью хакера были компьютеры с установленным на них программным обеспечением «Банк-Клиент». Технология была такова. Для заражения этих компьютеров и последующего хищения денег Виртальский использовал троянские программы типа Carber различных модификаций и, получив с их помощью логины, пароли и цифровые подписи, осуществлял платежи якобы от имени организаций или граждан на счета подставных фирм. Впоследствии он переводил деньги на пластиковые карты и обналичивал в банкоматах. Почти все зараженные компьютеры находились на территории России. Ежедневно вредоносные программы рассылались более чем миллиону «заинтересованных» лиц, в результате чего в отдельные дни заражалось свыше 100 тыс. компьютеров. За один раз Виртальскому удавалось завладеть сразу несколькими десятками миллионов рублей. На момент задержания хакера количество зараженных компьютеров составило около 6 млн, из них в основной бот-сети — 4,5 млн. Со счетов граждан и организаций похищено свыше 150 млн руб. Как квалифицировать действия Виртальского? Нет ли оснований для применения в этой ситуации ст. 159.6 УК?
13. Двадцатичетырехлетний математик, гражданин РФ Левин, изменив физический адрес технического устройства и использовав чужое имя, проник в компьютерную

систему Сити-банка (Англия) с целью хищения 2,8 млн. долларов. Своими действиями Левин блокировал на длительное время законного пользователя информации о движении финансовых средств банка и осуществил разрыв сети ЭВМ. Дайте уголовно-правовую оценку действий Левина. Когда считается оконченным состав данного преступления? Что характерно для субъективной стороны этого посягательства?

Шкала оценивания: 5-балльная.

Критерии оценивания:

5 баллов (или оценка «отлично») выставляется обучающемуся, если задача решена правильно, в установленное преподавателем время или с опережением времени, при этом обучающимся предложено оригинальное (нестандартное) решение, или наиболее эффективное решение, или наиболее рациональное решение, или оптимальное решение.

4 балла (или оценка «хорошо») выставляется обучающемуся, если задача решена правильно, в установленное преподавателем время, типовым способом; допускается наличие несущественных недочетов.

3 балла (или оценка «удовлетворительно») выставляется обучающемуся, если при решении задачи допущены ошибки некритического характера и (или) превышено установленное преподавателем время.

2 балла (или оценка «неудовлетворительно») выставляется обучающемуся, если задача не решена или при ее решении допущены грубые ошибки.

2 Оценочные средства для промежуточной аттестации обучающихся

2.1 Банк вопросов и заданий в тестовой форме

1. К сфере высоких технологий можно отнести:
○ интернет и компьютерные сети
○ трубопроводный транспорт
○ нефтедобывающую промышленность
○ государственное управление
2. К преступлениям в сфере высоких технологий можно отнести:
○ преступления в сфере компьютерной информации
○ транспортные преступления
○ преступления, связанные с оборотом наркотиков
○ преступления террористического характера
3. Первые компьютерные преступления были зафиксированы:
○ в конце 1960 годов
○ в конце 1950 годов
○ в конце 1940 годов
○ в конце 1980 годов
4. Первые нормы, устанавливающие ответственность за преступления в сфере высоких технологий, в российском уголовном законодательстве появились:
○ в 1996 году
○ в 1991 году
○ в 2001 году
○ в 2014 году
5. К новым угрозам в области высоких технологий не относятся:
○ заражение вредоносными программами отдельных компьютеров
○ информационные войны
○ атаки типа Distributed Denial of Service (DDoS)
○ использование компьютерных сетей для политических переворотов

6. В криминологическую характеристику преступности не входят:

○ признаки соответствующих составов преступлений

○ детерминанты (причины и условия) преступлений

○ статистические показатели преступности

○ характеристика личности преступника

7. Преступления в сфере высоких технологий связаны с использованием … закономерностей:

○ кибернетических

○ информационных

○ психологических

○ правовых

8. Наименее опасным является следующий тип личности киберпреступника:

○ случайный

○ ситуативный

○ злостный

○ особо злостный

9. Конвенция Совета Европы о преступности в сфере компьютерной информации:

○ не ратифицирована Россией, подпись отозвана

○ не подписывалась Россией

○ подписана и ратифицирована Россией

○ подписана, но не ратифицирована Россией

10. По образовательной, социальной и материальной характеристике личности киберпреступников они схожи с:

○ «беловоротничковыми» преступниками

○ профессиональными преступниками

○ насильственными преступниками

○ «ворами в законе»

11. В уголовном праве РФ преступные деяния должны обладать признаками:

○ общественной опасности и противоправности

○ только общественной опасности

○ только противоправности

○ общественной опасности и (или) противоправности

12. Основным федеральным законом, регулирующим информационный оборот в РФ, является:

○ Федеральный закон РФ «Об информации, информационных технологиях и защите информации»

○ Закон РФ «О средствах массовой информации»

○ Закон РСФСР «Об ответственности за правонарушения при работе с информацией»

○ Федеральный закон РФ «Об информации, информатизации и защите информации»

13. ФЗ «Об информации, информационных технологиях и защите информации» не регулирует отношения, связанные с:

○ защитой авторского права

○ применением информационных технологий

○ осуществлением права на поиск информации

○ обеспечением защиты информации

14. Право на поиск, получение, передачу, производство и распространение информации является:

○ конституционным

○ закреплённым в международных документах

○ закреплённым в федеральном законодательстве

○ не закреплённым в законодательстве

15. Информация в РФ может являться объектом отношений:

○ всех перечисленных
○ публичных
○ гражданских
○ административно-правовых
16. Возможность получения информации и её использования:
○ доступ к информации
○ защита информации
○ право на информацию
○ информационный оборот
17. Правом разрешать или ограничивать доступ к информации наделён:
○ обладатель информации
○ хозяин информации
○ собственник информации
○ оператор информационной системы
18. Обязанностью обладателя информации не является:
○ предоставление другим лицам доступа к информации
○ соблюдение прав и законных интересов других лиц
○ принятие мер по защите информации
○ ограничение доступа к информации в случаях, предусмотренных законом
19. К общеизвестной информации не относится:
○ персональные данные граждан
○ информация о состоянии окружающей среды
○ информация, накапливаемая в открытых фондах библиотек
○ информация об использовании бюджетных средств
20. От материи и энергии информация отличается следующим:
○ на неё не распространяются законы сохранения
○ она не может передаваться от одного объекта к другому
○ её понятие легко поддаётся определению через другие понятия
○ информация существует только в сознании людей
21. Отличительным признаком компьютерной информации, согласно УК РФ, является:
○ представление в форме электрических сигналов
○ хранение в машинночитаемой форме
○ обработка в компьютерах
○ передача через компьютерные сети
22. Признаком информационно-телекоммуникационной сети не является
○ подключение к Интернету
○ доступ с использованием средств вычислительной техники
○ использование линий связи
○ предназначенность для передачи информации
23. Неправомерным является доступ к информации, осуществляемый:
○ без ведома и разрешения её обладателя
○ с нарушением работы компьютера
○ только в нарушение прямо установленного в законе запрета
○ путём использования специальной программы («эксплоита»)
24. Последствием неправомерного доступа к компьютерной информации не является:
○ нарушение работы ЭВМ, системы ЭВМ, их сети
○ копирование информации
○ модификация информации
○ блокирование информации
25. Не может рассматриваться как результат неправомерного доступа к компьютерной информации:

○ стирание информации с магнитного диска при помощи магнита
○ внесение изменений в информацию без ведома её обладателя
○ установка препятствий для доступа обладателя и иных пользователей к информации
○ копирование информации на другой носитель

26. Обязательным признаком состава неправомерного доступа к компьютерной информации являются
○ преступные последствия
○ способ
○ место
○ предмет преступления

27. Квалифицирующим признаком неправомерного доступа к компьютерной информации не является его совершение:
○ с использованием специальных технических средств
○ из корыстных побуждений
○ с причинением крупного ущерба
○ группой лиц по предварительному сговору

28. Крупным ущербом применительно к неправомерному доступу к компьютерной информации признаётся ущерб, превышающий:
○ 1 миллион рублей
○ 250 тысяч рублей
○ 1,5 миллиона рублей
○ 6 миллионов рублей

29. Лицом, использующим служебное положение, в ст. 272 УК РФ не может быть признан:
○ программист, имеющий доступ к информационной системе
○ должностное лицо
○ государственный служащий
○ руководитель коммерческой организации

30. К тяжким последствиям, предусмотренным ч. 4 ст. 272 УК РФ, может быть отнесено:
○ всё перечисленное
○ причинение тяжкого вреда здоровью людей
○ наступление аварий и катастроф
○ серьёзное нарушение деятельности организаций

31. Использование чужих учётных данных для доступа к сети Интернет, причинившее ущерб 1200 рублей, квалифицируется:
○ преступлением не является, влечёт административную ответственность
○ по ст. 165 УК РФ («причинение имущественного ущерба путём обмана или злоупотребления доверием»)
○ по совокупности ст. 165 УК РФ и ст. 272 УК РФ
○ по ст. 272 УК РФ («неправомерный доступ к компьютерной информации»)

32. Криминологической особенностью неправомерного доступа к компьютерной информации не является:
○ крайняя редкость случаев совершения данного преступления
○ высокая латентность
○ значительная профессионализация данного вида преступности
○ наличие среди преступников лиц, не имеющих специального образования

33. Неправомерный доступ может осуществляться к информации:
○ любого характера
○ составляющей охраняемую законом тайну
○ конфиденциального характера
○ перечень видов такой информации определяется Правительством РФ

34. Признаком вредоносной программы не является:
○ способность к самостоятельному размножению и распространению («вирус»)
○ совершение действий без согласия пользователя
○ выполнение уничтожения, блокирования, модификации или копирования информации
○ существование в объективной форме
35. Статья 273 УК РФ предусматривает ответственность за создание:
○ компьютерных программ и иной компьютерной информации, обладающих вредоносными свойствами
○ только вредоносных компьютерных программ
○ только иной информации
○ нет правильного ответа
36. Вредоносная программа может существовать:
○ только в форме выполняемого программного кода
○ только в форме исходного программного кода
○ как в форме выполняемого, так и в форме исходного кода
○ в форме программного кода или в виде идеи алгоритма
37. В число преступных действий, предусмотренных ст. 273 УК РФ, не входит:
○ приобретение программы
○ распространение программы
○ создание программы
○ использование программы
38. Обязательным признаком состава ст. 273 не являются:
○ преступные последствия
○ преступное деяние
○ вина в форме прямого умысла
○ предмет — компьютерная программа, обладающая определённым свойствами
39. Видом вредоносной программы не является:
○ загрузчик информации
○ компьютерный вирус
○ троянский конь
○ логическая бомба
40. Не является признаком вредоносной программы:
○ нарушение работы компьютера и подключённого к нему оборудования
○ модификация информации
○ нейтрализация средств защиты информации
○ уничтожение информации
41. Использованием вредоносной программы признаётся:
○ её исполнение на компьютере
○ запись её на машинный носитель
○ компиляция исходного кода
○ анализ алгоритма программы
42. Использование вредоносных программ допускается российским законодательством:
○ не допускается ни в каких целях
○ в целях контроля за работниками со стороны работодателя
○ в целях раскрытия и расследования преступлений
○ для предотвращения нарушения авторских прав
43. Распространение вредоносной программы может осуществляться:
○ всеми перечисленными способами
○ путём её продажи
○ путём её безвозмездной передачи другому лицу

○ путём доведения её до всеобщего сведения в компьютерных сетях

44. Уголовный кодекс РФ не устанавливает ответственности за создание программ:

○ для массовой рассылки электронной почты (спама)

○ для обхода средств защиты информации

○ для блокирования доступа к компьютеру с требованием «выкупа»

○ для подмены содержимого интернет-сайтов, просматриваемых пользователем

45. Под правилами эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в уголовно-правовой литературе предлагается понимать:

○ всё перечисленное

○ техническую документацию на компьютерную технику

○ нормативные правовые акты, принимаемые органами государственной власти, например, санитарные нормы

○ локальные нормативные документы (правила внутреннего распорядка, должностные инструкции)

46. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей может быть совершено

○ как действием, так и бездействием

○ только путём бездействия

○ только активными действиями виновного

○ данный вопрос является спорным

47. Крупным ущербом в ст. 274 УК РФ («Нарушение правил эксплуатации...») признаётся ущерб, превышающий:

○ 250 тысяч рублей

○ 1 миллион рублей

○ 1,5 миллиона рублей

○ 3 миллиона рублей

48. Квалифицированный состав ч. 2 ст. 274 не предусматривает:

○ наступления особо крупного ущерба

○ причинения тяжких последствий

○ создание угрозы наступления тяжких последствий

○ нет правильного ответа

49. Ст. 274 УК РФ не предусматривает ответственность за нарушение правил эксплуатации:

○ средств вывода компьютерной информации

○ средств хранения компьютерной информации

○ информационно-телекоммуникационных сетей

○ оконечного оборудования

50. Обязательным признаком ст. 274 УК РФ («Нарушение правил...») является причинение:

○ крупного ущерба

○ значительного ущерба

○ тяжких последствий

○ существенного вреда

51. Преступным последствием в ст. 274 УК РФ («Нарушение правил...») не признаётся:

○ поломка средств компьютерной техники

○ копирование компьютерной информации

○ уничтожение компьютерной информации

○ блокирование компьютерной информации

52. Проблемой применения ст. 274 УК РФ («Нарушение правил...») является неопределённость содержания понятия:

○ правила эксплуатации указанных в статье объектов

○ компьютерная информация

○ крупный ущерб

○ блокирование информации

53. Деяние, предусмотренное ст. 274 УК РФ («Нарушение правил...») может совершаться со следующей формой вины:

○ неосторожность

○ умысел

○ умысел и неосторожность

○ только преступная небрежность

54. Состав ст. 274 УК РФ («Нарушение правил...»):

○ материальный

○ формальный

○ формально-материальный

○ усечённый

55. Причинная связь в ст. 274 УК РФ («Нарушение правил...») носит:

○ сложный характер (два взаимосвязанных последствия)

○ простой характер (одно последствие)

○ не является признаком данного состава преступления

○ особо сложный характер (более трёх взаимосвязанных последствий)

56. Особенностью нарушения авторских и смежных прав в компьютерных сетях не является

○ преимущественно возмездный характер незаконного распространения охраняемых объектов

○ массовый характер нарушений

○ безвозмездный характер распространения охраняемых объектов

○ отсутствие у большинства нарушителей злостных преступных установок

57. Образующей крупный размер нарушений авторских прав признаётся стоимость экземпляров произведений или прав на использование, превышающая:

○ 100 тысяч рублей

○ 250 тысяч рублей

○ 1 миллион рублей

○ 1,5 миллиона рублей

58. Образующей особо крупный размер нарушений авторских прав признаётся стоимость экземпляров произведений или прав на использование, превышающая:

○ 1 миллион рублей

○ 250 тысяч рублей

○ 1,5 миллиона рублей

○ 6 миллионов рублей

59. Незаконное использование объекта авторских прав может образовывать:

○ установка программы для ЭВМ на компьютер

○ адаптация законно полученного экземпляра программы для ЭВМ для работы его на конкретном аппаратном обеспечении

○ создание программы для ЭВМ, имеющей схожие функции с уже существующей

○ создание программы, нейтрализующей технические средства защиты авторских прав

60. Средством предупреждения преступлений, связанных с нарушением авторских и смежных прав, получившим распространение в России, является:

○ блокировка сайтов

○ прекращение доступа абонентов в сеть Интернет

○ широкие кампании по уголовному преследованию нарушителей
○ массовое предъявление гражданско-правовых исков

61. Предметами незаконного распространения в сети Интернет становятся следующие объекты авторских прав:
○ все перечисленные
○ литературные произведения
○ аудиовизуальные произведения
○ компьютерные программмы

62. Размещение охраняемого авторским правом произведения в сети Интернет может нарушить следующее исключительное право автора:
○ на доведение произведения до всеобщего сведения
○ на воспроизведение произведения
○ на прокат произведения
○ на распространение произведения

63. Квалифицирующим признаком нарушения авторских и смежных прав (ст. 146 УК РФ) не является:
○ совершение деяния группой лиц без предварительного сговора
○ использование лицом служебного положения
○ совершение деяния группой лиц по предварительному сговору
○ совершение деяния в особо крупном размере

64. Лицо, создавшее сайт для размещения торрент-файлов, несёт ответственность:
○ не несёт уголовной ответственности
○ по ст. 146 УК РФ («Нарушение авторских и смежных прав») как исполнитель
○ по ст. 146 УК РФ как пособник
○ по ст. 146 УК РФ как организатор

65. Лицо, использующее торрент-технологию для скачивания незаконно распространяемых объектов авторских прав, несёт ответственность по ст. 146 УК РФ:
○ потому что одновременно со скачиванием распространяет данные объекты
○ потому что использование торрент-технологий запрещено законом
○ не несёт ответственности
○ потому что приобретает контрафактный экземпляр произведения

66. Незаконное использование объектов авторского права (ч. 2 ст. 146 УК РФ) осуществляется со следующей формой вины:
○ прямой умысел
○ косвенный умысел
○ преступная небрежность
○ преступное легкомыслие

67. К способам хищения с использованием новых информационных технологий не относится хищение с использованием:
○ чужих банковских платёжных карт
○ систем «Интернет-банк»
○ неправомерного доступа к компьютерной информации
○ вредоносных программ

68. Уголовный кодекс РФ предусматривает ответственность за:
○ мошенничество в сфере компьютерной информации
○ вымогательство в сфере компьютерной информации
○ кражу с использованием компьютерной техники
○ присвоение или растрату с использованием компьютерной техники

69. Состав ст. 159.6 «Мошенничество в сфере компьютерной информации» по сравнению с основным составом мошенничества является:
○ привилегированным
○ квалифицированным

○ совпадающим по степени общественной опасности
○ эти составы не связаны между собой

70. Крупным размером в ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» признаётся стоимость имущества, превышающая
○ 1,5 миллиона рублей
○ 1 миллион рублей
○ 250 тысяч рублей
○ 3 миллиона рублей

71. С использованием новых информационных технологий не совершаются следующие преступления против собственности:
○ разбой
○ мошенничество
○ вымогательство
○ присвоение или растрата

72. Блокирование информации на компьютере с целью получения выкупа от её обладателя квалифицируется:
○ только по составам компьютерных преступлений (ст. 272, 273 УК РФ)
○ только как вымогательство (ст. 163 УК РФ)
○ по совокупности компьютерных преступлений и вымогательства
○ как компьютерное мошенничество (ст. 159.6 УК РФ)

73. Не могут являться предметом хищения:
○ денежные суррогаты (например, биткоины)
○ электронные денежные средства
○ деньги на платёжной карте
○ деньги на «личном счёте» в интернет-магазине

74. Мошенничество в сфере компьютерной информации не может совершаться путём:
○ использования чужой платёжной карты в банкомате
○ ввода компьютерной информации
○ вмешательства в функционирование средств хранения информации
○ модификации компьютерной информации

75. Мошенничество в сфере компьютерной информации следует квалифицировать:
○ вопрос о необходимости квалификации по совокупности однозначно не решён
○ по совокупности со статьями о компьютерных преступлениях
○ без совокупности со статьями о компьютерных преступлениях
○ только по статьям о компьютерных преступлениях

76. Криминологической особенностью хищений с использованием новых компьютерных технологий не является:
○ крайняя редкость их совершения
○ высокая латентность
○ массовость совершения
○ хищение как мелких, так и крупных сумм денег

77. Предметом хищения с использованием новых компьютерных технологий могут являться:
○ электронные деньги
○ объекты авторских и смежных прав
○ материальные объекты
○ виртуальные объекты

78. Определение понятия «порнография» в российском законодательстве содержится:
○ в законе «О защите детей от информации, причиняющей вред их здоровью и развитию»
○ в законе «О порнографии»
○ в законе «Об информации, информационных технологиях и защите информации»

○ в УК РФ

79. Распространение порнографических материалов через сеть Интернет:

○ является квалифицирующим признаком ст. 242 УК РФ

○ ненаказуемо

○ охватывается основным составом ст. 242 УК РФ

○ является административным правонарушением

80. Доходом в крупном размере в ст. 242 УК РФ «Незаконные изготовление и оборот порнографических материалов или предметов» признаётся доход, превышающий:

○ 50 тысяч рублей

○ 250 тысяч рублей

○ 1 миллион рублей

○ 1,5 миллиона рублей

81. Ключевым элементом определения порнографии является:

○ натуралистичность изображения или описания сексуальных отношений

○ направленность на вызов сексуального возбуждения

○ характер совершаемых сексуальных действий

○ субъекты совершаемых сексуальных действий

82. Для распространения порнографических материалов с изображением несовершеннолетних в настоящее время преимущественно используются:

○ анонимные сети (Tor, I2P)

○ файлообменники

○ торрент-сайты

○ социальные сети

83. Распространение порнографических материалов в сети Интернет:

○ запрещено в некоторых странах, в том числе России

○ разрешено повсеместно в мире

○ запрещено в некоторых странах, но не в России

○ запрещено повсеместно в мире

84. Уголовная ответственность по ст. 242 УК РФ не наступает за:

○ изготовление порнографических материалов в личных целях

○ продажу порнографических материалов

○ бесплатное распространение порнографических материалов

○ изготовление порнографических материалов с целью распространения

85. Создание интернет-сайтов, предлагающих посреднические услуги при занятии проституцией рассматривается как:

○ организация занятия проституцией (ст. 241 УК РФ)

○ административное правонарушение

○ ненаказуемое деяние

○ вовлечение в занятие проституцией (ст. 240 УК РФ)

86. Борьба с интернет-сайтами, распространяющими порнографию, затруднена вследствие:

○ их нахождения за пределами РФ

○ отсутствия определения порнографии в законодательстве РФ

○ отсутствия нормы, устанавливающей ответственность за распространение порнографии

○ использования анонимных сетей (Tor, I2P)

87. Отнесение материала к порнографическим осуществляется на основе:

○ заключения искусствоведческой экспертизы

○ заключения сексологической экспертизы

○ решения следователя

○ решения специализированного государственного органа

88. Что из перечисленного не является особенностью распространения порнографических материалов через сеть Интернет?

○ всё перечисленное является особенностью

○ бесплатный характер распространения

○ открытый характер распространения

○ высокая доля любительских материалов

89. Подлежат блокировке сайты, распространяющие:

○ порнографические материалы с изображением несовершеннолетних

○ порнографические материалы с участием животных

○ порнографические материалы, изображающие гомосексуальные отношения

○ любые порнографические материалы

90. К экстремистским материалам, размещаемым в сети Интернет, нельзя отнести:

○ критику действующих представителей власти

○ призывы к насильственному свержению действующей власти

○ призывы к насилию в отношении определённой социальной группы

○ материалы, возбуждающие ненависть в отношении определённой социальной группы

91. Террористические организации в своей деятельности используют:

○ всё перечисленное

○ анонимные сети (Tor, I2P)

○ электронную почту

○ электронные платёжные средства

92. Может рассматриваться как публичные призывы к осуществлению экстремистской деятельности:

○ всё перечисленное

○ размещение призыва на личной странице в социальной сети

○ размещение призыва в блоге

○ размещение призыва в открытом доступе на интернет-сайте, не являющимся блогом или СМИ.

93. Неправомерный доступ к компьютерной информации и использование вредоносных программ теоретически могут являться способом совершения следующих преступлений:

○ всех перечисленных

○ диверсия

○ террористический акт

○ шпионаж

94. При организации массовых беспорядков могут использоваться:

○ всё перечисленное

○ социальные сети

○ смартфоны, содержащие средства геолокации

○ mesh-сети

95. Публичные призывы к экстремистской деятельности, совершаемые с использованием сети Интернет, являются оконченными:

○ с момента ознакомления с призывами хотя бы одного лица

○ с момента ознакомления с призывами двух и более лиц

○ с момента ознакомления с призывами большого числа лиц

○ с момента размещения призывов

96. Криминологической особенностью размещения в сети Интернет информации экстремистского характера не является:

○ использование анонимных сетей (Tor, I2P)

○ массовый характер преступления

○ использование социальных сетей

○ объединение распространителей и адресатов информации в сообщества

97. Субъектами враждебной деятельности против РФ в Интернете могут выступать:

○ все перечисленные

○ частные лица

○ неправительственные организации

○ спецслужбы иностранных государств

98. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства может происходить по признакам:

○ всего перечисленного

○ пола

○ расы

○ сексуальной ориентации

99. Использование «высоких технологий» (в частности, сети Интернет) практически не характерно для преступлений:

○ против жизни и здоровья

○ в сфере экономической деятельности

○ против собственности

○ экстремистского характера

100. С использованием Интернета могут совершаться:

○ все перечисленные деяния

○ клевета

○ угроза убийством или причинением тяжкого вреда здоровью

○ сбыт наркотических средств

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36 или 60) и максимального балла за решение ситуационной задачи (6). Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение ситуационной задачи. Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по дихотомической шкале следующим образом:

Соответствие 100-балльной и дихотомической шкал

Сумма баллов по 100-балльной шкале	Оценка по дихотомической шкале
100-50	зачтено
49 и менее	не зачтено

2.2 Ситуационные задачи

1. В настоящее время большое распространение получили мошеннические схемы с использованием популярных сайтов объявлений, таких как «Авито», «Юла», «Циан» и иные интернет-площадки для размещения объявлений. Для общения с пользователями платформ мошенники использует «фейковые» интернет-страницы (зарегистрированные на выдуманное лицо), а также нелегально приобретенные сим-карты. Причем при использовании данных площадок для хищения чужого имущества мошенник может «примерить на себя» роль как продавца, так и покупателя.

В первой ситуации, лицо, имеющее умысел на завладение чужими денежными средствами, размещает в сети «Интернет» на соответствующей площадке объявление о продаже

какого-либо имущества, которым оно заведомо не владеет. После размещения объявления перед мошенником встает задача убедить позвонивших или написавших по данному объявлению граждан перевести ему денежные средства по предоплате. Для получения от потерпевших предоплаты мошенник обычно использует банковские карты, привязанные к текущим счетам, оформленным на иных лиц, зачастую не осведомленных о преступных намерениях мошенника (например, когда преступник обращается к лицам из маргинальных слоев населения с просьбой оформить банковский счет на их имя за вознаграждение). По получении оплаты мошенник обналичивает денежные средства через банкомат, а от самой банковской карты избавляется.

Получив денежные средства в качестве предоплаты, мошенник перестает выходить на связь и удаляет страничку с объявлением. Вместе с тем возможно и продолжение мошеннических манипуляций, когда преступник желает завладеть полной стоимостью «продаваемого» товара, а не только суммой предоплаты. Тогда им приобретается заведомо более дешевое имущество, чаще всего даже отдаленно не напоминающее предмет продажи, которое почтой отправляется потерпевшему под видом вещи из объявления с сообщением трек-номера для отслеживания посылки.

Так, по одному из уголовных дел, К., разместивший объявление о продаже GPS-навигатора стоимостью 18500 рублей, после получения предоплаты отправил потерпевшему грузики из свинца и игрушечный фотоаппарат.

Получивший трек-номер для отслеживания посылки потерпевший в этот момент зачастую теряет бдительность и переводит мошеннику оставшуюся сумму, не дожидаясь получения самой посылки и проверки ее содержимого. К тому моменту, как будет доставлена посылка, мошенник обналичивает полученные от потерпевшего денежные средства и распоряжается ими по своему усмотрению.

Во второй ситуации мошенник связывается с продавцом по одному из объявлений, размещенных в сети «Интернет» и высказывает желание приобрести его товар или услугу с готовностью внести задаток. С целью якобы внесения предоплаты мошенник просит продиктовать реквизиты банковской карты продавца. Реквизиты карты на деле используются для дальнейшего совершения покупки за счет потерпевшего на каком-либо интернет-сайте или для получения доступа к личному кабинету потерпевшего через средства дистанционного банковского обслуживания. Для подтверждения совершения операции, мошенник, ссылаясь на всю ту же необходимость отправки предоплаты, запрашивает у потерпевшего поступивший ему на абонентский номер SMS-код подтверждения транзакции. После ввода кода мошенник приобретает за счет потерпевшего какое-либо имущество либо, используя «мобильный банк», переводит денежные средства со счета потерпевшего.

Проанализируйте данный кейс. Какие особенности имеет данный вид мошенничества по сравнению с мошенничеством, не использующим информационные технологии? Какие обстоятельства могут затруднить раскрытие данного преступления? Нужно ли преступнику для совершения данного преступления обладать какими-либо специальными знаниями в сфере информационных технологий? Какие можно предложить пути предупреждения подобных преступлений?

2. Американская компания по производству игрушек Mattel стала жертвой уэйлинг-мошенничества. Киберпреступники, стоявшие за этой атакой, тайно контролировали компьютерные сети и коммуникации компании в течение нескольких месяцев до инцидента. После того как в компании было объявлено о назначении нового генерального директора, киберпреступники использовали личность нового генерального директора Кристофера Синклера (Christopher Sinclair) для совершения атаки. В частности, киберпреступники отправили электронное письмо от имени Кристофера Синклера, в котором просили получателя одобрить перевод на сумму три миллиона долларов в банк Вэньчжоу в Китае на счет китайского поставщика. Поскольку просьба поступила от генерального директора, сотрудница компании перевела деньги, но позже связалась с ним по этому поводу. Генеральный директор сказал,

что не давал никаких указаний о переводе денег. После этого компания Mattel связалась с правоохранительными органами США, Федеральным бюро расследований США, своим банком и правоохранительными органами Китая (Ragan, 2016). Время инцидента (деньги были переведены накануне праздника) позволило китайским властям вовремя заморозить счета до открытия банков, и компания Mattel смогла вернуть свои деньги.

Проанализируйте данный кейс. Какие особенности имеет данный вид мошенничества по сравнению с мошенничеством, не использующим информационные технологии? Какие обстоятельства могут затруднить раскрытие данного преступления? Нужно ли преступнику для совершения данного преступления обладать какими-либо специальными знаниями в сфере информационных технологий? Какие можно предложить пути предупреждения подобных преступлений?

3. Корниш и Кларк (Cornish and Clarke, 2003) предложили пять стратегий и 25 методов (по пять методов в каждой стратегии) для предупреждения и сокращения преступности. *Выберите один вид киберпреступности и вписать в нижеследующую таблицу методы обеспечения кибербезопасности, которые бы они использовали для предотвращения и/или сокращения такой киберпреступности.*

Увеличение усилий	**Увеличение рисков**	**Сокращение награды**	**Снижение числа провокаций**	**Устранение оправданий**
Защита объекта	Усиление охраны	Скрытие объектов	Снижение унылого настроения и стресса	Введение правил
Контроль доступа на объект	Содействие естественному надзору	Удаление объектов	Недопущение ссор	Размещение указателей
Контроль выхода	Снижение анонимности	Идентификация имущества	Снижение эмоционального возбуждения	Взывание к совести
Перенаправление правонарушителей	Использование управляющих на местах	Подрыв рынков	Нейтрализация давления со стороны коллектива	Содействие соблюдению законов
Средства/орудия контроля	Усиление формального наблюдения	Лишение выгод	Препятствование имитации	Контроль за наркотиками и алкоголем

4. В 2013 году Дэйв Эггерс (Dave Eggers) написал роман «Сфера» (The Circle) об антиутопическом обществе, в котором людям настоятельно рекомендуется вести полностью «прозрачную» жизнь в качестве единственного способа «настоящего существования». Такая полная прозрачность предполагает, помимо всего прочего, круглосуточное наблюдение за людьми и демонстрацию их жизни зрителям в режиме реального времени. По мотивам этого романа в 2017 году был снят художественный фильм.

Какие элементы описанного общества можно найти в современной реальной действительности? Каковы положительные черты данного общества? Какие отрицательные черты данного общества? Будет ли существовать преступность в таком обществе? Какие новые угрозы несёт создание и внедрение технологий наблюдения за человеком?

5. В 2005 году в сети стало быстро распространяться фото женщины под заголовком «Девушка с собачьей какашкой» в качестве способа унижения за то, что девушка не подобрала экскременты ее собаки в метро. Вскоре после того, как неизмененные фотографии были опубликованы, интернет-группы «бдительных» пользователей внимательно изучили фотографию, и через несколько дней ее личность была установлена, а ее личные данные опубликованы в Интернете. Фотография быстро стала одним из самых популярных поисковых запросов на популярных веб-порталах и источником пародии и насмешливой сатиры. Девушка была вынуждена отчислиться из университета и публично извиниться. Она пригрозила, что в случае, если «буллинг» продолжится, она засудит всех участвующих в нём, а «в крайнем случае» совершит самоубийство.

Нарушает ли эта практика права человека? Причиняет ли она страдания жертве? Является ли унижение мерой, соразмерной совершенному деянию? Можно ли привлечь за распространение такого фото к уголовной ответственности? Нужны ли какие-то правовые меры для предотвращения таких деяний?

6. В августе 2017 года тайский студент-активист был заключен в тюрьму на два с половиной года за размещение в «Facebook» статьи «Би-би-си», которая была сочтена оскорбительной для короля Таиланда. Он выложил в социальную сеть ссылку на статью «Би-би-си» на тайском языке, в которой описывалась биография короля, через два дня после инаугурации нового короля. Статью просмотрели более 2000 человек. Он был также обвинен в нарушении закона о компьютерных преступлениях. В соответствии с тайским законодательством оскорбление величества (lese-majeste) представляет собой тяжкое преступление против королевской семьи.

Является ли уголовное наказание за подобные деяния необходимым и соразмерным угрозе, которую представляет собой совершенное деяние? Нужно ли привлекать к какой-либо ответственности лиц, оскорбляющих представителей власти в Интернете? А оскорбляющих обычных людей?

7. Контролер компании Scoular.co, занимающейся торговлей сырьевыми товарами, предположительно получил электронные письма от имени генерального директора компании Чака Элси (Chuck Elsea) и базирующейся в штате Небраска аудиторской фирмы, которая сотрудничает с компанией, с просьбой об осуществлении трех банковских переводов в китайский банк на общую сумму около 17 миллионов долларов (Reuters, 2015). В электронных письмах содержалась просьба о сохранении конфиденциальности, поскольку деньги предназначались для приобретения китайской компании. Контролер выполнил требования, полагая, что письма отправил генеральный директор, хотя использованный адрес электронной почты не был официальным адресом электронной почты компании.

К какому типу киберпреступности относится это преступление? Пожалуйста, объясните свой ответ.

8. 1 марта 2022 года в интернете оказались доступны телефоны пользователей «Яндекс.Еды» и информация об их заказах. Утечку информации в сервисе подтвердили и объяснили: данные клиентов оказались в общем доступе из-за «недобросовестных действий одного из сотрудников». Уточнялось, что утечка не коснулась банковской информации, а также логинов и паролей. По итогам проверки, «Яндекс» заявил, что ужесточил подход к хранению чувствительной информации, исключил ее ручную обработку, и сократил сотрудников с доступом к ним минимум втрое. В конце марта интернет-пользователи заметили интерактивную карту, которая была построена на основе данных клиентов «Яндекс.Еды». На ней были выделены 58 тыс. адресов. После клика на любой из них высвечивались инициалы пользователя, его номер телефона, адрес электронной почты и общая сумма всех заказов. Тогда в компании заявили, что никаких новых утечек данных после 1 марта – не было. Карту с данными пользователей заблокировал Роскомнадзор.

Проанализируйте данный кейс. Что сделало возможным такую утечку данных — технические уязвимости или недостатки социального и правового регулирования? Как можно предотвратить подобные утечки. Кого надо привлекать к ответственности в связи с подобными утечками?

9. Программист городской больницы воспользовался доступом коллеги к Единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ), чтобы незаконно получить сертификат о вакцинации от коронавируса и QR-код для себя и своих родственников. Поскольку имелась в виду двухкомпонентная вакцина, то через 21 день были проделаны аналогичные действия.

Параметры доступа программист узнал, когда коллега, имевшая доступ к ЕГИСЗ, попросила его внести логин и пароль в настройки браузера: пароль был длинный и его сложно было запомнить.

История вскрылась, когда одному из родственников поступил проверочный вопрос из больницы, реально ли была пройдена вакцинация. Родственник был не в курсе ситуации и ответил отрицательно. После этого программист сам пришел к руководству и во всем сознался.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Может ли данное посягательство быть отнесено к посягательствам на критическую информационную инфраструктуру? Предложите квалификацию данного деяния. Сопоставьте данную квалификацию с предложенной при рассмотрении дела судом. Считаете ли вы правильным решение суда по данному делу?

Примечание: Кизилюртовский городской суд Республики Дагестан, Дело №1-148/2021. https://судебныерешения.рф/64233332

10. Сотрудник оборонного предприятия (выпускает заряды к реактивным системам залпового огня, комплексам ПВО, заряды двигателей для авиаракет, стартово-разгонные системы крылатых ракет, изделия для комплекса ПРО, сферические пороха для стрелкового оружия) решил помочь знакомой, уходившей на дистанционное обучение, найти активатор лицензии для офисного пакета известного производителя. Со служебного компьютера он скачал активатор. Он запустил его, решив его проверить на работоспособность, и «в нагрузку» получил вредоносную программу — «троянского коня», который попытался установить связь с IP-адресом, находящимся на территории США, что включило сигнал тревоги на межсетевом экране. Сотрудники службы безопасности предприятия и ФСБ установили источник угрозы и деактивировали вредоносную программу.

Было установлено, что антивирус на рабочем месте оказался просроченным и не обновленным. Было предположено также, что сотрудник специально внес в него исключение для запуска активатора, однако доказать это не удалось. Также было установлено, что передаваемая информация представляла собой сигнал типа heartbeat («я здесь, жду команды»), не содержащий никакой информации, обрабатываемой в информационной системе, а лишь свидетельствующий о работоспособности программы.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Может ли данное посягательство быть отнесено к посягательствам на критическую информационную инфраструктуру? Предложите квалификацию данного деяния. Сопоставьте данную квалификацию с предложенной при рассмотрении дела судом. Считаете ли вы правильным решение суда по данному делу?

Примечание: Кировский районный суд г. Перми, Дело №1-181/2021, https://судебныерешения.рф/60027623

11. Помощник машиниста ОАО «РЖД» решил пройти тестирование на получение допуска к выезду с помощью бота – специального ПО, предоставляющим тестируемому в модуле «АС ГРАТ» программного комплекса «АСУТ» ОАО «РЖД» получение положительного результата независимо от правильности ответов на вопросы теста. Он нашёл в Интернете сайт, где продавалась программа-бот, оплатил её стоимость в размере 520 рублей и скопировал на флешку. Бот с флешки был установлен, тестирование пройдено на "отлично", допуск получен.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Может ли данное посягательство быть отнесено к посягательствам на критическую информационную инфраструктуру? Предложите квалификацию данного деяния. Сопоставьте данную квалификацию с предложенной при рассмотрении дела судом. Считаете ли вы правильным решение суда по данному делу? Подлежат ли уголовной ответственности лица, создавшие и распространявшие программу-бота?

Примечание: Советский районный суд г. Волгоград, Дело №1-215/2021, https://судебныерешения.рф/59994592

12. Козлов, находясь в помещении компьютерного клуба, зашел на сайт видеохостинга YouTube, где просмотрел видеоинструкцию, рассказывающую о «взломе» сайтов. В описании видео была ссылка на скачивание программы, позволяющей проводить аудит безопасности удалённого информационного ресурса посредством загрузки и запуска данной программы. Далее Козлов установил эту программу. В период с 10.27 по 10.30 часов Козлов, с целью проверки своих навыков по использованию программы, внёс в неё данные URL сайта "Омский образовательный портал" Департамента образования города Омска, после чего запустил программу. В результате программа выявила название используемого на сайте ПО системы менеджмента контента (CMS) и вывела список уязвимостей, которые могли бы

быть использованы для атаки на сайт. Фактические никакие уязвимости для атак использованы не были, последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации выявлено не было.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Может ли данное посягательство быть отнесено к посягательствам на критическую информационную инфраструктуру? Предложите квалификацию данного деяния. Сопоставьте данную квалификацию с предложенной при рассмотрении дела судом. Считаете ли вы правильным решение суда по данному делу? Подлежат ли уголовной ответственности лица, создавшие и распространявшие программу для поиска уязвимостей?

Примечание: Первомайский районный суд г. Омска, Дело № 1-398/2021, https://www.securitylab.ru/blog/personal/valerykomarov/351678.php

13. Сотрудники отдела «К» УВД г. Энска А. и З. для повышения показателей раскрываемости компьютерных преступлений решили провести «оперативный эксперимент». Найдя в газете бесплатных объявлений объявление об оказании услуг «компьютерной помощи», они позвонили давшему его Р. и попросили его оказать помощь в установке на компьютер программного продукта Autodesk Alias Surface 2016 (стоимость лицензии на который составляла 1 млн. 145 тыс. рублей). Поначалу Р. отказался, однако после повторных звонков и обещания дополнительного вознаграждения всё же согласился. Требуемую программу он скачал из Интернета, там же он нашёл средства, позволяющие обойти технические ограничения, связанные с защитой авторских прав. Для установки программы был подготовлен компьютер, содержащий «чистую» ОС Windows. После того, как Р. закончил установку и «взломал» программу, оперативники задержали его. Р. было предъявлено обвинение в покушении на совершение нарушения авторских и смежных прав в особо крупном размере, неправомерный доступ к компьютерной информации, совершённый из корыстной заинтересованности и причинивший крупный ущерб, а также в использовании вредоносных компьютерных программ, предназначенных для нейтрализации средств защиты компьютерной информации, совершённое из корыстной заинтересованности и причинивший крупный ущерб.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Правильна ли квалификация? Правомерны ли действия оперативников?

Примечание: приговор Лефортовского районного суда г. Москвы от 07 июня 2012 года

14. К., обнаружив в интернете сайт, на котором представители кавказских национальностей обсуждали способы знакомства с русскими девушками, движимый мотивом неприязни к лицам указанных национальностей, разместил на одном из популярных интернет-форумов своё описание ситуации, в котором в грубой форме с использованием матерной брани высказал мнение о неполноценности лиц указанных национальностей. К сообщению К. приложил ссылку на программу «Low Orbit Ion Cannon», предназначенную для организации интернет-атак типа «распределённый отказ в обслуживании» (DDoS) и инструкцию по её использованию для приведения в неработоспособное состояние указанного им сайта. Согласно записям в техническом журнале форума, программу скачали 2530 человек. В ходе следственных мероприятий была установлена личность 120 из них, доказать факт использования программы удалось в отношении 10. В результате атаки сайт не работал две недели, в результате перегрузки оборудования владельцу оборудования ООО «Самшит», на котором размещался сайт, был причинён ущерб 30 тысяч рублей, на восстановление сайта и перенос его на другой сервер его владельцем Г. было потрачено 50 тысяч рублей. Кроме того, Ч., один из пользователей форума, на котором К. разместил сообщение, подобрав пароль администратора сайта, скопировал личные данные 1300 пользователей сайта (электронные адреса,

пароли, анкеты для знакомств) и разместил их на том же форуме. Дайте полную юридическую оценку деяния.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Изменится ли решение задачи, если объектом атаки станет сайт органа власти муниципального образования (например, с целью мести за коррупционные действия муниципальных властей)?

15. Никонов и его жена Никонова находились в зарегистрированном браке, в течение которого совместно пользовались интернет-ресурсами. Никонов имел в своем распоряжении пароли, которые использовала Никонова при посещении интернет-сайтов. После расторжения брака Никонова указанные пароли не сменила, и не запрещала своему бывшему супругу использовать их, равно, как и не запрещала посещать используемые ранее ими обоими интернет-сайты. Никонов, с учетом сложившихся между ним и потерпевшей отношений после развода, использовал ранее известные ему пароли с целью обнародования факта их с Никоновой развода.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Предложите квалификацию данного деяния. Можно ли признать данное деяние малозначительным?

Примечание: апелляционное определение по делу №10-3958/2013 Московского городского суда

16. М. зарегистрировался на интернет-форуме и нашел на нем информацию о незаконном заработке посредством неправомерного доступа к электронным почтовым ящикам пользователей и привязанным к ним аккаунтам компьютерной игры «Танки Онлайн». После этого М. приобрел на маркетплейсе нелегальной информации в «даркнете» файл с информацией о логине и пароле электронного почтового ящика, принадлежащего потерпевшему Е. Затем М. вошел в этот почтовый ящик и изменил в нем пароль. Тем самым он получил неправомерный доступ к компьютерной информации об учетных данных личного кабинета Е. Используя данные электронной почты, М. вошел в аккаунт потерпевшего в виртуальной сетевой игре. Затем в личном кабинете пользователя игры М. изменил адрес электронного почтового ящика, привязанный к игровому аккаунту. После этого М. продал неустановленному лицу виртуальные игровые ценности (премиальные танки) персонажа аккаунта, принадлежащие Е., и распорядился полученными от продажи денежными средствами по своему усмотрению.

Проанализируйте данный кейс. Выявите признаки состава преступления в сфере компьютерной информации. Предложите квалификацию данного деяния. Сопоставьте данную квалификацию с предложенной при рассмотрении дела судом. Считаете ли вы правильным решение суда по данному делу?

Примечание: постановление Советского районного суда г. Нижнего Новгорода от 11.04.2017 по делу № 1–112/2017, https://sudact.ru/regular/doc/8fOXO0Qg7g5Q/

17. Инженер телекомпании Еленин создал торрент-трекер, на котором размещал доступные для скачивания кинофильмы, права на которые принадлежали российским и зарубежным компаниям. Обвинение было предъявлено по трём фильмам — "Операция Ы", "Титаник" и "Мальчишник-3". Копию последнего, снятую на телефон в кинотеатре, Еленин разместил на своем торрент-трекере задолго до официального релиза. В итоге правообладатели — киноконцерны "Мосфильм", 20th Century Fox и Warner Brothers оценили суммарный ущерб в 2,1 млн рублей. Еленину было предъявлено обвинение в незаконном использовании авторских и смежных прав в особо крупном размере.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как должен устанавливаться ущерб и размеры нарушения по таким делам? Правильна ли квалификация?

18. Молодой специалист ОАО «РЖД», работающий проводником на поездах дальнего следования, в качестве хобби занимается уже несколько лет изготовлением фотографий поездов и ж/д составов. Со временем ему удалось приобрести качественное фотооборудование, и снимки стали получаться не только высокого разрешения, но и хорошего качества. В рамках фотоконкурса, проводимого ОАО «РЖД», он отправляет сделанные фотоснимки пригородного поезда на станции Слюдянка на электронную почту ответственного за проведение конкурса Сотрудника. Спустя две недели, возвращаясь из очередной поездки, специалист обнаруживает, что в кассе Центрального вокзала Иркутска продаётся расписание следования пригородных поездов на будущий год с его фотографиями на обложке без указания авторства. Своего согласия на использование данных фотографий он не давал, в условиях конкурса также ничего об этом не сказано. Специалист считает, что его работы были использованы с нарушением авторского права, ведь целью отправки фотографий была победа в конкурсе.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как в данном случае установить размер нарушенных авторских прав?

19. В Управление "К" МВД России обратился представитель ООО "Фирма грамзаписи "Никитин", который сообщил о том, что в социальной сети "Вконтакте" происходит незаконное распространение аудиоматериалов, исключительные права на которые принадлежат указанной фирме. В ходе проверки, проведенной специалистами Управления "К", выяснилось, что одним из наиболее активных пользователей, осуществляющих незаконное воспроизведение и доведение до всеобщего сведения музыкальных произведений, является 26-летний житель г. Москвы. На своей персональной странице он разместил 18 аудиозаписей известной российской музыкальной группы, число скачиваний которых другими пользователями составило свыше 200 тысяч. Правообладатель, руководствуясь стоимостью отчислений, которые получает с аналогичных стриминговых сервисов за прослушивание одного трека, а также количеством прослушиваний, заявил о том, что понес ущерб в виде недополученной выгоды в размере 108 тысяч рублей. Деяние было квалифицировано по ч. 2 ст. 146 УК РФ как нарушение авторских прав в крупном размере.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как должен устанавливаться ущерб и размеры нарушения по таким делам? Правильна ли квалификация? Имеются ли основания для привлечения к уголовной ответственности (проанализируйте признаки субъективной стороны преступления)?

20. Б., А.А. и З. в составе организованной группы осуществляли на постоянной основе деятельность по незаконному проведению азартных игр вне игровой зоны с использованием игрового оборудования, на котором незаконно использовались игровые программы "BananasGoBahamas", "BookofRa", "Columbus", "DiamondTrio", "DolphinsPearl", "LuckyLady,sCharm", "MoneyGame", "QueenofHearts", "UltraHot", исключительные авторские права на которые принадлежат компании "NovomaticAG". Данные программы никогда на территории России официально не продавались, компания на территории РФ не работала, однако правоохранительные органы, получив информацию по запросу, выяснили стоимость программ в евро и посчитали, что правообладателю причинён материальный ущерб на общую сумму 614305 рублей 80 копеек, то есть в крупном размере.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как должен устанавливаться ущерб и размеры нарушения по таким делам?

21. Козлов, автор фитнес-методики для лица и созданных для ее продвижения материалов, обратился с заявлением в правоохранительные органы, попросив привлечь к уголовной ответственности конкурента Сидорова, продвигавшего в интернете схожий продукт. Было установлено, что действительно, в странице социальной сети Сидорова предлагается к приобретению техника выполнения физиологических упражнений, а также последователь-

ность таких упражнений, которые являются практически полностью совпадающие с техникой и методикой Козлова. Однако аудиовизуальные материалы, подготовленные Сидоровым для демонстрации техники, выполнены самостоятельно, не копируют материалы Козлова. Установлено, что Сидоров реализовал 25 комплексов по цене от 249 до 295 долларов США на общую сумму не менее 5000 долларов США. Козлов аналогичные комплексы продавал по цене 500 долларов США. Козлов заявил, что ему был причинен крупный ущерб в виде упущенной выгоды и уменьшения рынка сбыта легальной продукции.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как устанавливается крупный ущерб по делам о плагиате? Является ли фитнес-методика объектом авторских и смежных прав?

22. Ефремов, увидев в свободном доступе в интернете разработанный Голиковым электронный учебный курс ускоренного изучения иностранных языков (который на сайте Голикова продавался за 8000 рублей), скопировал его, модифицировал, указав автором себя и реализовывал как авторский через свои социальные сети. Стоимость «подписки на курс» у Ефремова составила 4000 рублей. Всего Ефремов подписал таким образом около 100 человек.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как устанавливается крупный ущерб по делам о плагиате?

23. Музыкант Алиев записывал «кавер-версии» хитов известных исполнителей и размещал их на своём канале на видеохостинге. Договоров об использовании произведений Алиев не заключал, отчислений в Российское авторское общество не делал. Было установлено, что Алиев получил от видеохостинга за размещение рекламы в его роликах 800 тысяч рублей. Кроме того, правообладатели музыкальных произведений сообщили, что суммарная стоимость прав на использование произведений таким образом, вычисленная по аналогичным договорам, заключённым с другими музыкантами, составила 1 миллион 600 тысяч рублей.

Проанализируйте данный кейс. Выявите признаки состава преступления. Является ли создание кавер-версии нарушением авторских прав? Изменится ли ответ, если будет выяснено, что Алиев исполнял не приближенные к оригиналу варианты произведений, а видоизменённые путём комической стилизации, целью которой являлось высмеивание характерных черт оригинальных произведений и манеры исполнителей?

24. Художник Кононов находил в интернете изобразительные работы, созданные различными пользователями с использованием нейросетей (см. пример в приложении). Затем он творчески дорабатывал данные работы, скрывая недостатки, присущие «компьютерному художнику», а также комбинировал элементы разных работ, создавая коллажи. Полученные работы он продавал на NFT-аукционе, получив в результате доход в криптовалюте, суммарно 1,5 биткоина (что по курсу на момент выявления данной схемы составляло 1 742 334.43 рублей). Установлено, что ни с программистами, осуществлявшими создание и обучение нейросети, ни с создателями изображений, которые осуществляли творческую работу по формулированию запроса и отбору предлагаемых нейросетью изображений, никаких договоров Кононов не заключал.

Проанализируйте данный кейс. Имеются ли здесь признаки нарушения законодательства? Может ли Кононов быть привлечён к уголовной ответственности? Являются ли использованные им работы объектами авторских и смежных прав? Как исчисляется ущерб при извлечении дохода в криптовалюте?

25. В ходе проводившегося в Красноярске турнира по игре CounterStrike одного из участников обманом выманили из здания, где проводился турнир. Там его, угрожая пистолетом, посадили в машину и, продолжая угрожать пистолетом, потребовали передать вирту-

альные предметы (ножи), которые были приобретены потерпевшим до этого за 27 тысяч рублей. Потерпевший выполнил на своём мобильном устройстве действия по передаче предметов с аккаунта игры, после чего был отпущен.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как должен устанавливаться ущерб и размеры нарушения по таким делам? Как может быть квалифицировано данное деяние?

26. Петр Пирон и Евгений Пригожин узнав, что гражданин Ш. имеет доступ к валютным счетам и занимается конвертацией криптовалюты в фиатные деньги, решили обмануть потерпевшего и завладеть его активами. Обладая информацией о том, что Ш. занимается управлением счетов и проведением конвертации криптовалюты разных видов, попытался путем обмана похитить у Ш. криптовалюту на сумму не менее 1 000 000 рублей, которой в последующем распорядится по своему усмотрению, в том числе путем продажи (обмена) за наличные деньги, для чего в названный период дважды встречался с другом Ш. – К., и, представляясь ему сотрудником ФСБ, сообщал ложную информацию о грозящей Ш. уголовной ответственности за его деятельность с криптовалютой, а также возможности избежать уголовной ответственности, если Ш. переведет на его электронные адреса криптовалюту в указанном им количестве. Когда добиться согласия на выдачу средств преступникам не удалось, они решили разыграть задержание Ш. Собрав группу из 5 человек Пирон и Пригожин выследили потерпевшего, похитили его прямо возле подъезда собственного дома и вымогали перевода биткоинов и фиатных денег на свои кошельки. Поддавшись на провокации и угрозы, потерпевший передал похитителям деньги: 5 млн. рублей и 99,70 биткоинов, что по курсу на дату совершения преступления составляло свыше 48 млн. рублей.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Что является предметом преступления? Как должен устанавливаться ущерб и размеры нарушения по таким делам? Как необходимо квалифицировать деяние?

27. В Казани Серяков, Кононов, Васильев и Захаров решили реализовать следующую преступную схему. Они находили жертву, желающую продать биткоины, путём просмотра объявлений на соответствующих форумах и площадках в Интернете. Затем они связывались с жертвой и предлагали купить криптовалюту по цене выше курса на криптовалютных биржах, после чего создавали видимость передачи денежных средств, взамен получая от потерпевшего перевод биткоинов на указанный кошелёк. Однако в одном из эпизодов они, при непосредственной встрече с жертвой, решили действовать следующим образом: представившись сотрудниками полиции, виновные усадили потерпевшего в автомобиль, пристегнули наручниками к поручню, и угрожая причинением вреда здоровью, заставили его разблокировать телефон, на котором была установлена программа управления криптовалютным кошельком, после чего сами совершили перевод криптовалюты в размере 4,2867 биткоина, что по курсу на дату совершения преступления составило 14805919 рублей.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Что является предметом преступления? Как должен устанавливаться ущерб и размеры нарушения по таким делам? Как необходимо квалифицировать деяние?

28. Сотрудники центрального аппарата ФСБ России Архаров и Козлов, работавшие в отделе по расследованию преступлений в сфере высоких технологий, потребовали от Окулова, обвинённого в двух эпизодах мошенничества в особо крупном размере, передать им биткоины под угрозой назначения максимально строгого наказания. В случае получения биткоинов они обещали содействовать в частичном прекращении уголовного дела и смягчении назначенного наказания. Потерпевший передал им 4,74023 биткоина, что по курсу на дату совершения преступления составило 16372375 рублей.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как должен устанавливаться ущерб и размеры нарушения по таким делам? Как следует квалифицировать деяние?

29. Сотрудники вычислительного центра банка «Уникум» Каталов, Арбузов и Григорьев, имея доступ к компьютерной программе учета, ведения и оформления банковских операций отдела текущих счетов, изменили ее таким образом, что она позволяла округлять размеры платежей, а разницу перечислять на счет, открытый женой Каталова. Затем жена Каталова сняла со счета деньги в размере 120 тыс. руб., которые Каталов, Арбузов и Григорьев поделили поровну.

Проанализируйте данный кейс. Выявите признаки состава преступления. Кому причинён ущерб, кто является потерпевшим по данному делу? Как следует квалифицировать содеянное?

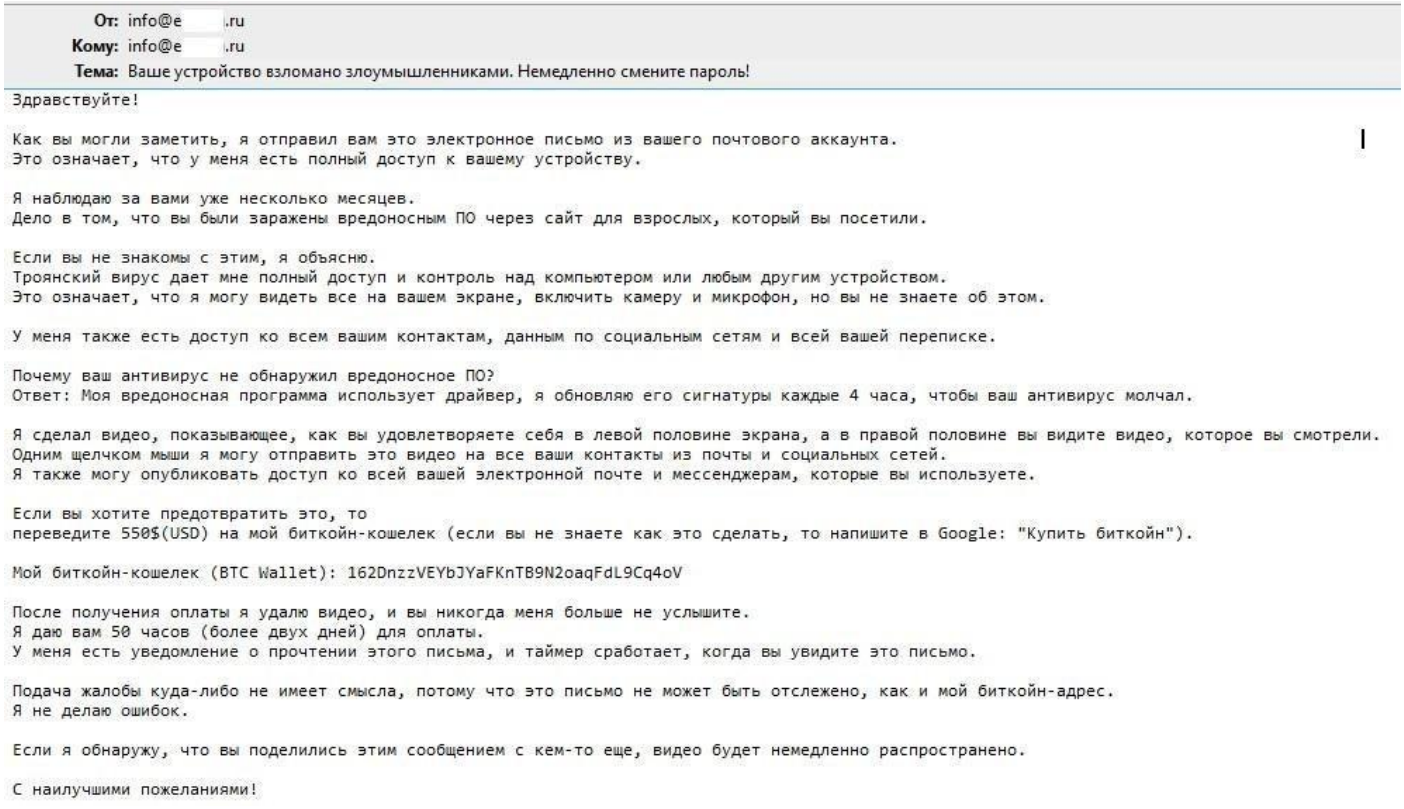
30. 22-летний Виртальский специализировался на создании хакерских программ. Он не только создавал бот-системы и массово распространял вредоносные программы, но и лично принимал участие в хищении денег с различных счетов. Мишенью хакера были компьютеры с установленным на них программным обеспечением «Банк-Клиент». Технология была такова. Для заражения этих компьютеров и последующего хищения денег Виртальский использовал троянские программы типа Carber различных модификаций и, получив с их помощью логины, пароли и цифровые подписи, осуществлял платежи якобы от имени организаций или граждан на счета подставных фирм. Впоследствии он переводил деньги на пластиковые карты и обналичивал в банкоматах. Почти все зараженные компьютеры находились на территории России. Ежедневно вредоносные программы рассылались более чем миллиону «заинтересованных» лиц, в результате чего в отдельные дни заражалось свыше 100 тыс. компьютеров. За один раз Виртальскому удавалось завладеть сразу несколькими десятками миллионов рублей. На момент задержания хакера количество зараженных компьютеров составило около 6 млн, из них в основной бот-сети — 4,5 млн. Со счетов граждан и организаций похищено свыше 150 млн руб.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как необходимо квалифицировать деяние?

31. 18 апреля 2022 киберпреступники группировки Conti, часть из которых являлась гражданами Российской Федерации, атаковали сервера министерства финансов и науки, инноваций, технологий и телекоммуникаций Коста-Рики. Некоторые из государственных цифровых платформ были заражены вымогательским ПО Conti. В руки хакеров попали более терабайта баз данных, переписок и внутренних документов. Сразу после атаки Conti опубликовали заявление, в котором пообещали раскрыть «тайны министерства», так как «министр не может сам объяснить налогоплательщикам, что происходит». Они обещали публиковать внутренние документы, базы налогоплательщиков и другие данные. В обмен на молчание хакеры потребовали у правительства 10 миллионов долларов в биткоинах. В результате в Коста-Рике было объявлено чрезвычайное положение, целый ряд правительственных организаций был вынужден вернуться к доцифровым технологиям работы.

Проанализируйте данный кейс. Выявите признаки состава преступления. Следует ли квалифицировать данное только как преступление против собственности или есть основания для применения иных составов преступления?

32. Калистратов получил по электронной почте письмо следующего содержания, якобы отправленное с его собственного e-mail адреса:



От: info@e .ru
Кому: info@e .ru
Тема: Ваше устройство взломано злоумышленниками. Немедленно смените пароль!

Здравствуйте!

Как вы могли заметить, я отправил вам это электронное письмо из вашего почтового аккаунта.
Это означает, что у меня есть полный доступ к вашему устройству.

Я наблюдаю за вами уже несколько месяцев.
Дело в том, что вы были заражены вредоносным ПО через сайт для взрослых, который вы посетили.

Если вы не знакомы с этим, я объясню.
Троянский вирус дает мне полный доступ и контроль над компьютером или любым другим устройством.
Это означает, что я могу видеть все на вашем экране, включить камеру и микрофон, но вы не знаете об этом.

У меня также есть доступ ко всем вашим контактам, данным по социальным сетям и всей вашей переписке.

Почему ваш антивирус не обнаружил вредоносное ПО?
Ответ: Моя вредоносная программа использует драйвер, я обновляю его сигнатуры каждые 4 часа, чтобы ваш антивирус молчал.

Я сделал видео, показывающее, как вы удовлетворяете себя в левой половине экрана, а в правой половине вы видите видео, которое вы смотрели.
Одним щелчком мыши я могу отправить это видео на все ваши контакты из почты и социальных сетей.
Я также могу опубликовать доступ ко всей вашей электронной почте и мессенджерам, которые вы используете.

Если вы хотите предотвратить это, то
переведите 550$(USD) на мой биткойн-кошелек (если вы не знаете как это сделать, то напишите в Google: "Купить биткойн").

Мой биткойн-кошелек (BTC Wallet): 162DnzzVEYbJYaFKnTB9N2oaqFdL9Cq4oV

После получения оплаты я удалю видео, и вы никогда меня больше не услышите.
Я даю вам 50 часов (более двух дней) для оплаты.
У меня есть уведомление о прочтении этого письма, и таймер сработает, когда вы увидите это письмо.

Подача жалобы куда-либо не имеет смысла, потому что это письмо не может быть отслежено, как и мой биткойн-адрес.
Я не делаю ошибок.

Если я обнаружу, что вы поделились этим сообщением с кем-то еще, видео будет немедленно распространено.

С наилучшими пожеланиями!

Поскольку Калистратов действительно посещал сайты для взрослых, он счёл содержание письма соответствующим действительности. Опасаясь, что разглашение подробностей его частной жизни может расстроить его свадьбу, которая вскоре должна была состояться, Калистратов заплатил злоумышленникам. Однако, как впоследствии разъяснил Калистратову приглашённый им специалист по информационной безопасности, данное письмо представляет собой массовую рассылку, организованную с целью обмануть и запугать получателей. Заголовок сообщения подделан, никаких вредоносных программ на компьютере Калистратова не было обнаружено. Калистратов обратился в полицию.

Проанализируйте данный кейс. Выявите признаки состава преступления. О каком преступлении или их комбинации здесь идёт речь?

33. Известный футболист Бадзюн познакомился на интернет-сайте с девушкой. В какой-то момент общение приобрело интимный оборот: новая знакомая предложила заняться «киберсексом» по видеосвязи. Бадзюн согласился, совершив перед камерой действия сексуального характера. Однако вскоре с ним связался неизвестный, сообщив, что за удовольствие надо заплатить, и потребовал 10 миллионов рублей, сказав, что в противном случае видео будет распространено в интернете. Бадзюн отказался. Через некоторое время видеоролик действительно был опубликован и быстро распространился по интернету. В результате пострадала спортивная карьера Бадзюна: он был вынужден оставить позицию капитана сборной.

Проанализируйте данный кейс. Выявите признаки состава преступления. Следует ли квалифицировать данное только как преступление против собственности или есть основания для применения иных составов преступления?

34. Ф. начал создавать и наполнять контентом группы в социальной сети ВКонтакте, которые впоследствии стали известны как «суицидальная секта». В них Ф. нагнетал депрессивные настроения и рассказывал о самоубийствах. Он неоднократно публиковал видео, в которых инсценировал свою смерть через повешение. Также он занимался организацией суицидальной «игры»: находя по «хештегам» желающих участвовать в игре, он выдавал им «номерки» и «задания», включавшие задания, требовавшие от подписчиков просыпаться

поздно ночью и решать задания-головоломки, просматривать депрессивного содержания видео, совершать акты самоповреждения. В основном участниками «игры» были подростки. Для большинства из них подобные игры являлись не более чем источником «острых ощущений», и с ними игра завершалась на имитации самоубийства — подростки выкладывали на свои страницы фотографии с высотных зданий, железных дорог, с порезами на венах и несколько дней не заходили в социальные сети. Фактически никаких деструктивных действий эти подростки не совершали. Однако с некоторыми потерпевшими, которых Ф. считал склонными к совершению самоубийства, работа продолжалась. Ф. внушал им решимость совершить суицид, описывал способы совершения самоубийства. Одной из жертв, девочке 17-летнего возраста, Ф. приказал снять на видео расправу над животным. Она отказалась убивать, после чего Ф. предложил ей покончить жизнь самоубийством, в противном случае пообещав убить её родителей (на деле возможности выполнить такую угрозу у него не было). Потерпевшая совершила покушение на самоубийство, но была спасена медиками. Свою мотивацию Ф. объяснил так: «Пространство во вселенной забито! Мы чистим мир от биомусора!». В ходе проведенной психолого-психиатрической экспертизы Ф. был признан вменяемым.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как может быть квалифицировано данное деяние?

35. В 2020 году в сети стало быстро распространяться видео женщины под заголовком «Вези меня мразь». На нем видно, как миловидная женщина (позже была установлена её личность — это оказалась Я., работавшая инструктором в фитнес-клубе) ведет себя откровенно неподобающим образом, истерит и оскорбляет таксиста, угрожает ему расправой. Запись сразу начинается с момента, когда Я. истерично орет, - «Вези меня на место, мразь. Меня люди ждут. Вези меня, тварь». После этого она начинает колотить водителя руками, а тот лишь успевает отбиваться и спрашивать: «Что вы делаете?». Потом оскорбления приобретают национальный оттенок, Я. начинает оскорблять уроженца Средней Азии, и обвинять его в том, что он специально не повез ее сразу, так как она русская. Увидев, что ее снимают на сотовый телефон, женщина бросается с кулаками на водителя и выбивает гаджет из рук, на чем запись обрывается. Причиной конфликта, как оказалось, стал сущий пустяк, когда таксист подъехал, Я. долго не выходила из подъезда и к сумме за поездку прибавилось 57 рублей за ожидание. После этого пассажирка и устроила скандал, отказавшись платить и тогда водитель отказался продолжать движение, попросив ее покинуть салон.

Видеозапись инцидента растиражировали многие федеральные СМИ, что привело к тому, что Я. Была вынуждена уволиться с работы. Сама «модель» позже признала, что вела себя неподобающим образом, и принесла извинения за свое поведение, сказав, что перенервничала, так как боялась опоздать на встречу. Сожаление случившимся выразил и сам водитель, сливший видеозапись в интернет, и явно не ожидавший столь широкой огласки. Я. подверглась интернет-травле: на ее страницы в социальных сетях был устроен настоящий «набег» возмущенных пользователей. Я. была вынуждена закрыть свои аккаунты, которые использовала в том числе для заработка.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

36. 1 марта 2022 года в интернете оказались доступны телефоны пользователей «Яндекс.Еды» и информация об их заказах. Утечку информации в сервисе подтвердили и объяснили: данные клиентов оказались в общем доступе из-за «недобросовестных действий одного из сотрудников». Уточнялось, что утечка не коснулась банковской информации, а также логинов и паролей. По итогам проверки «Яндекс» заявил, что ужесточил подход к хранению чувствительной информации, исключил ее ручную обработку, и сократил сотрудников с доступом к ним минимум втрое. В конце марта интернет-пользователи заметили интерактивную карту, которая была построена на основе данных клиентов «Яндекс.Еды». На ней были вы-

делены 58 тыс. адресов. После клика на любой из них высвечивались инициалы пользователя, его номер телефона, адрес электронной почты и общая сумма всех заказов. Тогда в компании заявили, что никаких новых утечек данных после 1 марта – не было. Карту с данными пользователей заблокировал Роскомнадзор.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

37. Группа пользователей одной из «имиджборд» (анонимных площадок для общения) при помощи сервиса FindFace, пытающегося найти среди пользователей соцсети ВКонтакте похожего по изображению лица, стали анализировать кадры из порнороликов и эротических фотосессий для разоблачения личности девушек. В случае, если аккаунт во «ВКонтакте» удавалось идентифицировать, ссылки на интимные видео и фото рассылались родственникам и друзьям порноактрис. Всего в подобной деятельности участвовало более 100 человек. В большинстве случаев всё ограничивалось закрытием страниц в соцсети, однако одна девушка (по национальности чеченка) была убита родственниками за то, что «опозорила семью», а одна совершила самоубийство, причём выяснилось, что на самом деле она в порно не снималась, а актриса просто на неё очень похожа.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать деяние?

38. В дежурную часть одного из отделов полиции Ленинградской области от гражданки поступило заявление о привлечении к уголовной ответственности неизвестного ей лица, которое с мая по июнь того же года, используя сеть Интернет, совершало развратные действия в отношении ее малолетней дочери посредством демонстрации фотографий обнаженных мужских половых органов, сопровождая их текстовыми сообщениями с предложениями о совершении действий сексуального характера за денежное вознаграждение в размере 10 тыс. руб.

В ходе предварительного следствия мать малолетней потерпевшей дала показания, что после просмотра ею страницы своей дочери в социальной сети "ВКонтакте" и обнаружения указанных фотографий она сообщила об этом своему мужу и обратилась к сотрудникам правоохранительных органов, после чего было принято решение продолжить переписку от имени дочери для того, чтобы договориться о встрече с мужчиной. В продолженной на странице дочери переписке ею намеренно допускались орфографические ошибки и мужчине целенаправленно было дано понять, что с ним переписывается малолетняя девочка, ученица 2 класса. Несмотря на то что мужчине стало достоверно известно, что пользователь, с которым он переписывается, является малолетней девочкой, он продолжал переписку и демонстрацию порнографических фотографий, спрашивал, нравятся ли они девочке, продолжал предлагать встречу с целью совершения действий сексуального характера за денежное вознаграждение, назначил место и время встречи в одном из населенных пунктов Ленинградской области и явился на встречу, где по результатам проведенного комплекса оперативно-розыскных мероприятий по подозрению в совершении преступления и был задержан сотрудниками полиции.

Подозреваемым оказался К. - 40-летний безработный, не имеющий семьи и детей, ранее не судимый житель г. Санкт-Петербурга, имеющий в соответствии с заключением экспертов, проводивших комиссионную судебно-психиатрическую экспертизу (в части заключения сексолога), признаки расстройства сексуального поведения в форме педоэфебофилии.

В тот же день по месту его проживания проведен обыск, в ходе которого изъят системный блок и CD диски, содержащие упомянутые фотографии, а также информацию о его переписке с малолетней потерпевшей и другими лицами женского пола с предложениями встретиться для совершения действий сексуального характера за денежное вознаграждение.

Примечание: http://lexandbusiness.ru/view-article.php?id=6972

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать содеянное?

39. После сетевого матча в игре Call of Duty, в котором победил М., а проиграл К., К. обиделся на М. и пригрозил последнему, что вызовет полицию на его адрес. М. заявил, что не боится и назвал адрес. Тогда К. позвонил в правоохранительные органы, используя сервис IP-телефонии с подменой номера, и сообщил, что из-за проигрыша в онлайн-игре он убил отца, взял в заложники мать с младшим братом и разлил по дому бензин, готовясь поджечь. Он также сообщил адрес, названный М. По указанному адресу выехала группа СОБР, имевшая при себе табельное оружие. Из-за двери действительно раздавались крики неясного характера и звуки ударов. Выбив дверь, СОБРовцы обнаружили 33-летнего Ж., который, увидев их, с криком бросился в сторону сотрудников. Было применено табельное оружие, Ж. причинён тяжкий вред здоровью. В результате разбирательства выяснилось, что М. назвал К. не свой адрес, а адрес Ж., жившего в соседнем подъезде. Ж. злоупотреблял алкоголем и в нетрезвом состоянии вёл себя шумно, постоянно устраивая скандалы с участием собутыльников и своей сожительницы. Один из таких скандалов с дракой происходил и в момент описанных событий. При этом Ж. не имел намерения нападать на представителей власти, а пытался выбежать из квартиры.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как необходимо квалифицировать деяние?

40. Супруги Т. как-то поссорились и хотели было разводиться, жена съехала. Муж на короткое время сошелся с К., которая прислала ему легкомысленный снимок на пляже без верхней части купальника.

Позже Т. помирился с женой, а та нашла в почте супруга, к которой имела доступ, изображение полуголой К. Т. решила, как потом сказала мужу, «проучить любовницу и дать понять, что никаких отношений с мужем у нее быть не может». Для этого она загрузила интимное фото К. «Вконтакте» с подписью, что та оказывает интимные услуги за деньги.

К. обратилась в полицию с заявлением о нарушении тайны ее интимной жизни. Как потерпевшая рассказывала в своих показаниях, она не давала Т. согласия показывать кому-либо эту фотографию, они об этом говорили. Она жаловалась, что ее репутация пострадала, о ней разошлась дурная слава, ей звонили мужчины, которым нужны были «услуги».

Проанализируйте данный кейс. Выявите признаки состава преступления. Следует ли квалифицировать данное только как преступление против неприкосновенности частной жизни или есть основания для применения иных составов преступления?

41. К. и М. организовали в соцсети ВКонтакте группу «Зацеперское сообщество». Они собирали в ней информацию по теме «трейнсёрфинга» (проезду на железной дороге снаружи подвижного состава), выкладывали фото и видео. Постепенно в группе образовалось устойчивое сообщество численностью в несколько сотен человек, в котором сформировались свои традиции и правила этики, организовывались массовые мероприятия по катанию снаружи поездов группами численностью в несколько десятков человек, координируемые через сообщество. Участники сообщества активно занимались вовлечением в него новых членов (среди которых значительную долю составляли несовершеннолетние), восхваляя своё увлечение и убеждая в его относительной безопасности. Правоохранительные органы заинтересовались деятельностью сообщества после смерти двух несовершеннолетних, которые, вдохновившись его материалами, решили снять видеоролик о путешествии на крыше электрички.

Проанализируйте данный кейс. Выявите признаки состава преступления. О каком преступлении или их комбинации здесь идёт речь?

42. Т. взломал компьютерную сеть водозабора № 1 в Челябинске и, получив доступ к управлению промышленным оборудованием, осуществил действия, направленные на остановку технологических процессов очистки и дезинфекции воды, что могло привести к попаданию загрязнённой воды в водопровод. Выяснилось, что Т. — бывший работник водокана-

ла, уволенный «по статье» за употребление спиртных напитков на рабочем месте. Вариант 1: действия совершены Т. с целью мести руководству водоканала. Вариант 2: Т. действовал по поручению анархической организации «Рассвет» с целью устрашить население и дезорганизовать деятельность органов власти. Вариант 3: Т. действовал по заданию разведки иностранного государства и преследовал цель подрыва экономической безопасности РФ за счёт вывода из строя стратегического объекта.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как может быть квалифицировано данное деяние?

43. На одном из магистральных газопроводов в отдалённой местности произошёл мощный взрыв. Специалистами было выяснено следующее. На газопроводе использовалась программное обеспечение для автоматизации технологических процессов (SCADA) производства компании, находящейся в Канаде. Программа, в частности, управляла насосами, турбинами и другими ключевыми элементами системы перекачки газа. После введения в отношении России санкций, данная компания отказалась исполнять контракты и заблокировала работу программного обеспечения. Для возобновления работы ПО специалисты отдела информационных технологий нашли на сайте, зарегистрированном на Каймановых островах, программу-«взломщик», которая позволяла обойти проверку, установленную поставщиком ПО. Оказалось, что на самом деле «взломщик» представляет собой «троянского коня», подготовленного при участии спецслужб США. Данная программа содержала код, обнаруживающий, что он работает на российском газопроводе, однако данный код не активировался при работе в обычном режиме. Соответственно, программа некоторое время работала нормально и была введена в эксплуатацию. Однако при отработке одного из режимов тестирования встроенный вирус привёл к нештатному режиму работы оборудования, что привело к разрыву газопровода и последующему взрыву.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

44. Аспирантка кафедры истории общественных движений и политических партий Исторического факультета МГУ Л. опубликовала в научном журнале статью «Теоретическое обоснование политического терроризма партии социалистов – революционеров», посвящённую деятельности указанной политической партии в начале XX века, включавшей организацию политически мотивированных взрывов, преследовавших цели убийства чиновников, дезорганизации деятельности органов власти и подъёма населения на бунт. В статье автор делает вывод о том, что действия террористов были обусловлены «реакционной политикой царского правительства» и являлись формой народно-освободительной борьбы.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

45. В нескольких телеграм-каналах, позиционирующих себя как «имеющих информаторов в органах власти» было опубликовано сообщение о том, что начиная с 1 января 2023 года, фиксация нарушений правил дорожного движения будет проводиться не только с помощью видеокамер, но и устанавливаемой во многих новых автомобилях отечественной навигационной системы ЭРА-ГЛОНАСС, которая поможет установить факты парковки в неположенном месте и превышения скорости. Утверждалось, что система ЭРА-ГЛОНАСС сможет автоматически фиксировать и передавать данные в Федеральный центр организации дорожного движения из любой точки страны, где доступна навигация. Данная информация была растиражирована в других социальных медиа и даже попала в некоторые федеральные СМИ. Автомобилисты стали обращаться в автосалоны с просьбой убрать из их автомобиля эту систему, а несколько человек даже вышло с плакатами «Нет шпионскому ГЛОНАССу» к Государственной Думе РФ. В итоге выяснилось, что первоисточником информации стало сообщение «информационного агентства Панорама», которое публикует вымышленные са-

тирические новости, о чём предупреждает у себя на сайте в форме сообщения под каждой новостью «Все тексты на этом сайте представляют собой гротескные пародии на реальность и не являются реальными новостями».

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать деяние?

46. В городском сообществе ВКонтакте был опубликован пост информационного характера, в котором говорилось о том, что некоторые трамвайные маршруты, не пользующиеся большой популярностью, в ближайшее время будут ликвидированы. Некоторые пользователи в комментариях высказались в поддержку данных, сказав, что «трамвай не нужен». Другие пользователи, являющиеся сторонниками сохранения трамвая, в грубой форме и с использованием бранной и нецензурной лексики вступили в спор. В частности, были зафиксированы следующие высказывания: «это ты [совсем] никому не нужен», «те, кому не нужен трамвай, не люди», «тех, кому не нужен трамвай, на фарш», «противников трамвая повесить на трамвайных проводах», «в трамвае ездят только [психически нездоровые] бабки и [лица с ослабленными умственными способностями]», «противники трамвая — конченые [пассивные гомосексуалисты]». Согласно статистическим данным сети ВКонтакте, сообщение и комментарии были просмотрены более 1000 раз. Один из прочитавших комментарии, З. обратился в отдел «Э» МВД России с просьбой проверить комментарии к сообщению на предмет наличия в них призывов к насилию в отношении социальной группы и унижения человеческого достоинства по признаку принадлежности к социальной группе.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать содеянное?

47. В конце 2000-х годов в среде имиджборд (анонимных сайтов для обмена изображениями и общениями) начало формироваться сообщество Anonymous, основанное на идеалах анонимности и свободы в Интернете. Изначально концепция «Анонимус» трактовалась как децентрализованное интернет-сообщество, действующее анонимно и скоординированно, для достижения своих целей, как правило, ради развлечений, связанных с различным интернет-юмором и мемами.

Постепенно идеология сообщества начала трансформироваться: стали появляться лица и группы лиц, осуществляющие различного рода кибератаки (против организаций, осуществляющих борьбу с нарушениями авторских прав, производителей средств кибербезопасности и интернет-ресурсов государственных органов, осуществляющих «цензуру»). Anonymous стал символом «хактивизма» — использования компьютерных атак для достижения политических целей. Более поздними целями анонимного хактивизма были правительственные учреждения Соединенных Штатов, Израиля, Туниса, Уганды и других; Исламское государство; сайты с детской порнографией; баптистская церковь Вестборо; и такие корпорации, как PayPal, MasterCard, Visa и Sony. Связанные группы LulzSec и Operation AntiSec осуществили кибератаки на правительственные учреждения США, СМИ, компании, военных подрядчиков, военнослужащих и сотрудников полиции.

У Anonymous нет единого лидерства и членства в привычном понимании. Как говорят представители движения, «любой, кто хочет, может быть Анонимус и двигаться к определённому набору целей». По словам экспертов, любой может быть его частью. Это толпа людей, работающих вместе и делающих что-то вместе для различных целей.

Проанализируйте данный кейс. Оцените применимость норм об организованной преступности к децентрализованным коллективам, подобным Anonymous.

48. И. приобрёл в магазине дистанционно управляемый беспилотный квадрокоптер DJI Mavic, оснащённый камерой и возможностью передачи изображения на смартфон. В домашних условиях он доработал «дрон», снабдив его кустарным приспособлением, позволяющим по команде оператора сбросить груз, прикреплённый к беспилотнику (массой до 1

кг). Затем он выставил дрон на продажу на площадке-аукционе в даркнете, указав, что он может быть использован, например, для доставки наркотиков или взрывчатых веществ.

Проанализируйте данный кейс. Есть ли признаки состава преступления? Как необходимо квалифицировать деяние?

49. На форуме игры «Танки Онлайн» один из пользователей опубликовал документы, описывающие характеристики бронебойного снаряда для одного из представленных в игре танков. В доказательство их подлинности он привёл собственные расчёты, по которым разработчики якобы должны изменить танк. Кроме того, на снимке он положил поверх документа сам снаряд. Документы были оперативно удалены с сайта, однако в журналах доступа сохранилась информация о том, что до этого момента к ним успел обратиться кто-то с IP-адреса, принадлежащего Центральному разведывательному управлению США. Выяснилось, что чертежи разместил инженер завода, выпускающего снаряды, имеющий оформленный в установленном порядке допуск к составляющим государственную тайну сведениям о характеристиках снаряда. Опубликованные сведения соответствовали засекреченным.

Проанализируйте данный кейс. Выявите признаки состава преступления. О каком преступлении или их комбинации здесь идёт речь? Как изменится ответ, если выяснится, что сведения были опубликованы военнослужащим одной из частей, на вооружении которой находятся снаряды, который не имел допуска к секретным сведениям, а характеристики снаряда выдумал сам?

50. У. создал в зоне .onion анонимной сети Tor сайт — торговую площадку. Функционал площадки позволял производить между продавцами и покупателями безопасные сделки с использованием криптовалют. Покупатели регистрировались на сайте бесплатно, а продавцы обязаны были покупать аккаунт через аукцион, чтобы уменьшить риск мошенничества. В магазине продавалось более 10 тысяч товаров, 70 % из них запрещённые во всех или большинстве стран психоактивные вещества (340 видов), самыми популярными из которых являлись МДМА, ЛСД и марихуана. Опиоиды, например, героин также имелись в продаже, однако спрос на них был крайне низкий. Правила магазина запрещали продажу детской порнографии, данных банковских карт, заказы убийств, оружия массового поражения. На сайте также продавалось небольшое количество товаров, оборот которых не запрещен, например книги, ювелирные изделия, порнография. Ежегодные продажи через сайт оценивались в 14—15 миллионов долларов. У. был задержан после того, как заказал на своём сайте поддельные документы — посылка была обнаружена и контролировалась полицией.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как может быть квалифицировано данное деяние?

51. В аэропорту «Домодедово» задержали двух девушек С. и К. (21 и 19 лет), которые пытались перевезти в Турцию свою подружку Л. (которой недавно исполнилось 18). Как выяснилось, Л. увидела в новостях сюжет, как кто-то пытался продать девственность. В разговоре с подругами она упомянула, что с мужчинами еще никогда не встречалась и за большие деньги была бы не прочь продать такой «товар». Среди подруг была та С. Через какое-то время она рассказала об этом разговоре своей подруге по модельному бизнесу К. Оказалось, что К. состояла в закрытых чатах в Telegram, где представители богатых мужчин ищут для них временных спутниц. На сообщение К. с предложением «экзотического» «товара» откликнулся потенциальный клиент. Переписка длилась несколько недель. По запросу клиента девушку из Серпухова нужно было переправить в Турцию. С «покупателем» она должна была встретиться уже там. Девушки объявили цену — 1,5 млн рублей. Миллион рублей должна была получить сама девственница, по 250 тысяч — ее посредницы. Л. привезли в «Домодедово», купили ей билет на самолет. Однако, как только представитель клиента передал С. и К. деньги, из засады появились оперативники, которые задержали девушек.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

52. Приехав в Москву в командировку К. решил развлечься и нашел на интернет-сайте объявление об оказании услуг проституции. Связавшись с «дамой», К. перевел по указанным реквизитам предоплату в размере 2 тысяч рублей — и принялся ждать гостью, предвкушая приятное времяпрепровождение. Однако девушка всё не приезжала и не приезжала. Тогда мужчина позвонил «администратору», номер которого был указан на сайте, и поинтересовался, почему возникла загвоздка. Тот объяснил, что аванса в две тысячи рублей мало для получения услуги, и потребовал еще денег. Вознамерившись во что бы то ни стало получить услугу, К. перевел еще 29 тысяч рублей. На ситуацию это не повлияло: «ночная бабочка» по-прежнему не спешила радовать клиента своим присутствием. Возмущенный слесарь вновь позвонил «администратору» и получил гневную отповедь: своими денежными переводами он якобы «сломал кассу» компании и причинил крупные убытки, которые должен возместить. Молодому человеку пригрозили, что, если он не перечислит «сутенерам» еще 185 тысяч рублей, приедут киллеры и жестоко расправятся с ним самим и всеми его родными. К. испугался и оформил кредит, чтобы выплатить «долг». Когда он отдал деньги, «администраторы» потребовали еще 500 тысяч под очередным надуманным предлогом — и с новыми угрозами. После этого, осознавая, что достать денег больше неоткуда, Андрей, наконец, заявил о случившемся в полицию.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

53. Безработный житель Новокубанска С. придумал хитроумный способ заработка по телефону. Он опубликовал на интернет-сайте анкету девушки Виктории, а когда «запавшие» на неё клиенты звонили по указанному номеру, пользовался программами по изменению голоса. Это позволяло ему говорить чужими голосами сначала от имени самой Виктории, потом её менеджера-сутенёра. Так, например, одним из потерпевших оказался житель Уфы Н. Позвонив по номеру анкеты, он договорился с «девушкой» о встрече. Н. вновь позвонил, когда приехал по указанному адресу, и получил в ответ просьбу внести две тысячи рублей в качестве предоплаты. Мужчина засомневался и спросил, не обманет ли она его. После этого девушка перевела разговор на своего «менеджера, который представился Кириллом. Он убедил потерпевшего перевести предоплату. После Кирилл потребовал еще 8400 рублей как гарант того, что с девушкой ничего не произойдет. Мужчина перечислил и эту сумму. Однако менеджеру «Виктории» и этого было мало. Он сказал клиенту, что у него проблемы с переводом, и нужно отправить еще денег. Под разными предлогами мошенник выпросил у несчастного еще несколько тысяч рублей – в конечном счете у мужчины вообще закончились свободные средства. Однако Н. был настроен решительно и намерен был во что бы то ни стало воспользоваться услугами конкретной девушки. Для этого он поехал в Казань, взял там деньги в кредит, отдав свой авто под залог, и перевел их на счет незнакомцу. Всего мужчина отдал злоумышленнику порядка 143 тысячи рублей. Всего С. таким образом «заработал» более 3 млн рублей.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать деяние?

54. Пенсионер К. обзавёлся компьютером и доступом в Интернет и начал постепенно осваивать новый для него виртуальный мир. Он зарегистрировался в социальной сети «Одноклассники», где выкладывал свои фотографии и писал сообщения. В одной из групп социальной сети он прочитал, что для того, чтобы бесплатно смотреть фильмы и сериалы, можно воспользоваться программой Shareaza. Установив данную программу, К. действительно быстро освоил поиск нужных ему боевиков и комедий. Заинтересовался он и фильмами «для взрослых». Он нашёл «коллекцию» одного из пользователей программы и скачал её. Среди

загруженных файлов оказался один, название которого на первый взгляд представляло собой бессмысленную комбинацию из букв и цифр. Файл оказался содержащим сцену полового акта с явно малолетней девочкой. К. ужаснулся, увидев содержимое, и сразу удалил файл.

Однако через некоторое время к нему пришли сотрудники полиции. Оказывается, скачивание данного файла было отслежено, а комбинация из букв и цифр представляет собой «маркеры», которые используются для обозначения «детской порнографии». Кроме этого, как сообщили К. сотрудники полиции, скаченный в Shareaza файл сохраняется на компьютере пользователя. Если компьютер подключен к сети интернет, любой пользователь программного продукта Shareaza может без ведома владельца получить доступ к внутренним папкам и скачать файлы. Фактически скачивания с компьютера К. осуществлено не было, но какое-то время файл был доступен другим пользователям.

К. вину не признал, указав, что не знал ни о содержании файла, ни об этой особенности программы.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать содеянное?

55. Полиция Санкт-Петербурга осуществила операцию по пресечению деятельности пяти вебкам-студий, модели которых проводили интим-трансляции для иностранцев. Задержано было 11 человек. В числе подозреваемых: 32-летний организатор, его 31-летняя помощница, подыскивающая персонал, 36-летний помощник — системный администратор, 42-летний помощник по вопросам, связанным с обеспечением безопасности, а также семь девушек-администраторов вебкам-студий в возрасте от 20 до 25 лет. Также было установлено, что над созданием контента в сети трудились 107 моделей, в том числе несовершеннолетние. Концепция работы проста. Любой желающий может виртуально купить за токены (электронная валюта) понравившуюся девушку и онлайн провести с ней время. Во время обысков в студиях правоохранители изъяли 54 мобильных телефона, пять станций удаленного управления, документацию с инструкциями, графиком и учетом рабочего времени моделей, а также пистолет и боеприпасы. На стене также висела табличка: «Приведи подругу – получи 7000 рублей». В целом, по оценкам полицейских, на онлайн-трансляциях студиям удалось заработать более 200 млн рублей. В то же время, никаких видеозаписей порнографического характера, изготовленных в студиях, обнаружено не было — работа осуществлялась исключительно в режиме прямой трансляции.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать содеянное?

56. «Треш-стример» Р., занимавшийся прямой трансляцией через Интернет «эпизодов из жизни», включавших употребление алкоголя, матерную брань, насилие и издевательства, решил устроить очередное «шоу». Сам «блогер» и его друзья употребляли алкоголь. На заднем плане все время присутствовала девушка в короткой одежде. Р. и его друзья издевались над девушкой в прямом эфире, били её, а в какой-то момент ей брызнули в лицо из перцового баллончика. Девушка начала жаловаться, а потом вообще задыхаться. В отместку Р. выгнал ее на улицу. Дело происходило в декабре, на улице был мороз. Через какое-то время Р. вспомнил о девушке и затащил её обратно в дом, так как она теряла сознание. Затем Р. начал понимать, что произошло что-то плохое — пытался привести девушку в чувство. Когда она перестала подавать признаки жизни, Р. вызвал скорую. Приехавшие сотрудники скорой констатировали летальный исход сразу же по приезду. При этом камера продолжала работать, пока на пороге не появились вызванные врачами полицейские. Они велели Р. прекратить трансляцию, заметив: «Всё, достримился». Судмедэкспертиза выявила у погибшей закрытую черепно-мозговую травму, множественные кровоподтёки и субдуральную гематому, которая образовалась в результате не менее трёх ударов по лицу.

Проанализируйте данный кейс. Есть ли признаки состава преступления? Как необходимо квалифицировать деяние?

57. В 2004 г. в России появилось виртуальное сообщество «чайлдфри» — людей, пропагандирующих добровольный отказ от деторождения, объединившее в своих рядах почти 500 человек. К 2014 году количество участников было 5000 человек. На сегодняшний день, в социальной сети «Вконтакте» число участников данной группы возросло до 15 тысяч человек. Сообщество имеет собственный интернет-сайт, на котором изложены принципы чайлдфри, главными из которых является бездетность по убеждению. Представители сообщества занимаются активной пропагандой бездетности. Среди них выделилось отдельное подсообщество «чайлдхейт», представители которого активно ненавидят детей. Их раздражает крик, плач, гиперактивность детей. В материалах, которые размещают представители сообщества в социальных сетях, часто встречаются высказывания, говорящие о превосходстве чайлдфри и унижающие честь и достоинство женщин-матерей, а некоторые высказывания содержат рассуждения о необходимом насилии над детьми.

Проанализируйте данный кейс. Есть ли признаки состава преступления? Как необходимо квалифицировать деяние?

58. Проходящее испытания на дорогах общего пользования беспилотное транспортное средство на базе автомобиля Volvo сбило насмерть велосипедистку, которая пересекала дорогу. Столкновение произошло в 2 часа ночи, в тёмное время суток. Женщина с велосипедом переходила дорогу, находясь за пределами пешеходного перехода, но при этом шла параллельно с ним, не наступая на разметку. За рулём автомобиля находился водитель, но сама машина находилась в режиме «автопилот» и двигалась со скоростью 60 км/ч.

При расследовании выяснилось, что за 5,6 секунд системы заметили помеху на пути: сперва машина не поняла, как человек может оказаться на трассе без транспортного средства. Вместо того, затормозить, ИИ в течение нескольких секунд пытался идентифицировать препятствие. Система несколько раз переквалифицировала помеху между «машиной» и «другое», и в итоге остановилась на варианте «велосипед». К этому моменту до столкновения осталось всего 1,2 сек. Еще секунду автомобиль рассчитывал вероятность столкновения и в конце концов применил торможение лишь за 0,2 сек до столкновения. В результате беспилотник наехал на женщину и нанёс ей несовместимые с жизнью травмы. Было также установлено, что инженеры производителя системы беспилотного управления отключили автоматическую систему безопасности Volvo, чтобы та не мешала работе ИИ. Эксперты заключили, что устройство беспилотника было построено ошибочно.

Согласно установленным правилам тестирования, когда на дороге возникают опасные ситуации, водитель обязан перехватить управление автомобиля, полностью взяв контроль над транспортным средством на себя. Других пассажиров в автомобиле не было. На записях с камер, установленных внутри беспилотника, было видно, что водитель поднимал глаза на дорогу «примерно 32 процента времени», а в остальное время смотрел «на консоль в районе правого колена». Проанализировав данные о трафике смартфона водителя, следователи выяснили, что в течение 40 минут вплоть до момента столкновения на телефон транслировалось шоу «Голос».

Проанализируйте данный кейс. Выявите признаки состава преступления. Как может быть квалифицировано данное деяние? Кто должен понести ответственность?

59. Федерацией шахмат Москвы был организован шахматный турнир с участием робота Chesserobot, который представляет собой управляемую шахматным компьютером рукуманипулятор, способную самостоятельно переставлять фигуры на доске. Робот играл на турнире сразу три партии с детьми. Среди его соперников был семилетний мальчик К. В партии с ним рука робота выполнила ход и «съела» фигуру на столе мальчика, поставив на это место свою фигуру. В это время произошла непредвиденная ситуация. К. чуть поторопился и начал делать ответный ход. Робот быстро отреагировал на движения мальчика неправильным образом. Машина буквально ухватила его указательный палец и сильно сдавила. Взрослые, кото-

рые были рядом, кинулись на помощь мальчику только через несколько секунд. Они остановили робота и вытащили палец Кристофера. Позже врачи зафиксировали у мальчика перелом фаланги и наложили гипс. По заключению эксперта, ребёнку был причинён лёгкий вред здоровью.

В ходе расследования выяснилось, что робот-шахматист собран на основе манипулятора производства компании Kuka Robotics, предназначенного для использования на промышленных конвейерных линиях. Конструкция зажима манипулятора использовала металлические элементы, на которые не были установлены мягкие прокладки. Усилие, развиваемое зажимом, явно превышало необходимое для удержания шахматной фигуры. Кроме того, на роботе отсутствовали сенсоры безопасности, останавливающие его при опасном приближении руки или какой-либо другой части тела человека.

Организаторы турнира утверждали, что сам ребёнок нарушил правила техники безопасности, потянувшись к фигуре до того, как рука манипулятора была убрана. Однако доказательств того, что с участниками турнира вообще проводился инструктаж по технике безопасности представлено не было.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние? Кто должен нести ответственность — производитель робота, организатор турнира или оба?

60. В генетической лаборатории был получен новый генетически модифицированный сорт дрожжей. Как и обычные дрожжи, они питаются сахаром, но синтезируют из него не этиловый спирт, а соединения, которые могут быть использованы при производстве лекарственных препаратов на основе морфина, используемых как сильные обезболивающие. По словам учёных, «выведших» данный сорт, его использование позволяет отказаться от использования в качестве сырья натурального мака, выращивание которого вызывает интерес наркопотребителей.

Через некоторое время после того, как информация об этом была опубликована в СМИ, из лаборатории было похищено около 100 г дрожжевой культуры. Как выяснилось по записям камер наблюдения, похищение совершил технический работник лаборатории К., действовавший по заданию преступного сообщества, занимавшегося производством синтетических наркотиков. Преступники рассчитывали культивировать дрожжевую культуру и продавать «наборы» по производству наркотиков на основе аппаратов для домашнего пивоварения.

Впрочем, оказалось, что генетики предвидели такую возможность. Цепочка генетических модификаций дрожжей включала в себя этап, на котором в них встраивался ген, делающий их воспроизводство возможным только в присутствии определённого химического вещества, формула которого держится в секрете и которое не является доступным для потребителя, а производится только для нужд химических предприятий под строгим контролем. Так что использовать дрожжи для производства наркотиков вне контролируемых лабораторных условий оказалось невозможно.

Проанализируйте данный кейс. Есть ли здесь признаки состава преступления? Как необходимо квалифицировать деяние?

61. В отделе кадров крупной транснациональной корпорации как один из этапов отбора соискателей на различные должности использовалась их оценка самообучаемой программой, работающей по принципу нейронной сети. Предполагалось, что программа будет беспристрастно оценивать личные и деловые качества кандидатов на основе анализа их резюме и доступных о них данных в иных источниках (в том числе закрытых базах данных этой корпорации).

Однако при анализе статистических данных выяснилось, что программа вместо беспристрастной оценки выдаёт весьма странные результаты: при оценке кандидатов на одни должности она отдавала предпочтение женщинам (процент отказа соискателям-мужчинам

составлял 87%, а женщинам — всего 22%), на другие — наоборот, мужчинам, на третьи она набирала лиц определённой национальности, на четвёртые — имеющих накопления существенного объёма и т.д.

При выяснении причин таких отклонений оказалось, что при обучении программы использовались личные дела работников, уже занимавших соответствующие должности. В итоге программа оценивала не профессиональную пригодность конкретного работника, а его соответствие профилю тех, кто до него принимался на данную должность. В итоге несмотря на то, что руководство корпорации хотело внедрением данной программы сгладить исторически сложившиеся перекосы, основанные на предвзятых представлениях о том, что на определённых должностях лучше работать женщинам или, напротив, мужчинам, на деле оно добилось только укоренения этих перекосов.

При анализе результатов работы программы выяснилось, что дискриминации подверглось не менее 100 человек, чьи профессиональные качества вполне позволяли занять соответствующие должности.

Проанализируйте данный кейс. Выявите признаки состава преступления. Как следует квалифицировать деяние? Кто должен понести ответственность?

Шкала оценивания решения ситуационной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение ситуационной задачи – 6 баллов. Балл, полученный обучающимся за решение ситуационной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по дихотомической шкале следующим образом:

Соответствие 100-балльной и дихотомической шкал

Сумма баллов по 100-балльной шкале	Оценка по дихотомической шкале
100-50	зачтено
49 и менее	не зачтено

Критерии оценивания решения ситуационной задачи:

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблон-

ного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.