Критерии оценивания.

Проверка олимпиадных работ осуществляется по заданиям. В каждом задании комиссия проверяет ответ, а также правильность, самостоятельность и полноту решения.

Ответ без объяснения не оценивается.

В случае неверного ответа за задание выставляется 0 баллов.

В случае, если решение задания выполнено с нарушением п. 29 Порядка проведения олимпиад школьников, за задание выставляется 0 баллов.

Математический блок и Кейс.

- Приведены верный ответ и полное обоснованное решение задачи: максимальный балл.
- Баллы могут быть снижены за арифметические ошибки или неполноту объяснений.

Гуманитарный блок.

- Приведён полностью верный ответ (выбраны все верные варианты ответа и ни одного лишнего): максимальный балл.
- В задании 1.2
  - ▶ за каждый выбранный верный вариант ответа начисляется 1 балл;
  - ▶ за каждый выбранный неверный вариант ответа снимается 1 балл.
- В задании 2.3
  - ▶ приведён полностью верный ответ — максимальный балл;
  - ▶ допущена одна ошибка (указан неверный наряду со всеми верными или отсутствует верный наряду со всеми остальными верными) — 1 балл;
  - ▶ в иных случаях — 0 баллов.
- В задании 3.3
  - ▶ за каждый выбранный верный вариант ответа начисляется 1 балл;
  - ▶ за каждый выбранный неверный вариант ответа снимается 1 балл;
  - ▶ выбор элементов 5 и 6 не влияет на оценку, их можно как указать, так и пропустить.

Математический блок. Задание 8.1 (5 баллов).

Старшеклассник Петя, желая быстро заработать и не зная об уголовной ответственности за неправомерный оборот электронного средства платежа, отозвался на объявление о поиске сотрудников для «тестирования нагрузки на платёжную систему» и согласился стать дропом. По указанию, поступившему в чате, он зарегистрировал один электронный кошелёк для получения средств и далее каждые 12 минут из каждого уже созданного кошелька он отправлял по 2 ссылки, ведущие на регистрацию новых кошельков, и активировал их.

Система финансового мониторинга инициирует проверку, как только количество кошельков, зарегистрированных с одного IP–адреса, достигает 60. Через какое время (в минутах) с момента регистрации первого электронного кошелька Петя будет обнаружен?

Примечание: все регистрации происходят мгновенно, а все кошельки автоматически привязываются к Петиному IP–адресу.

Ответ: 48 минут.

Решение. За одну итерацию из каждого созданного кошелька отправляются две ссылки, по которым активируются новые кошельки. Обозначим X_k количество зарегистрированных кошельков через k таких итераций. По условию $X_0 = 1$. Каждый раз количество увеличивается в 3 раза: $X_k = 3X_{k-1}$. Найдём несколько последовательных значений:

$$X_0 = 1;\ X_1 = 3 \cdot 1 = 3;\ X_2 = 3 \cdot 3 = 9;\ X_3 = 3 \cdot 9 = 27;\ X_4 = 3 \cdot 27 = 81.$$

После четырёх итераций число зарегистрированных Петей кошельков становится больше 60. Одна итерация занимает 12 минут. Значит, Петя будет обнаружен через $4 \cdot 12 = 48$ минут.

Математический блок. Задание 8.2 (5 баллов).

Служба финансовой безопасности крупной корпорации анализирует риски потери средств при проведении электронных транзакций. Система защиты имеет два независимых канала уязвимости (А и Б). Экспертная оценка определила вероятности возникновения финансовых потерь по каждому из каналов следующим образом.

– В связи с уязвимостью внутреннего сервера (канал А): от $0,1$ до $0,2$.

– В связи с возможным сбоем платёжного шлюза (канал Б): от $0,15$ до $0,25$.

Реализация угроз по разным каналам происходит независимо. На основании этих данных оцените снизу и сверху вероятность того, что у корпорации возникнут финансовые потери.

Ответ: $[0,235;\ 0,4]$.

Решение. Обозначим события M «*возникнут финансовые потери*», M_1 «*финансовые потери возникнут в связи с каналом А*» и M_2 «*потери возникнут в связи с каналом Б*». Потерь не будет, если они не возникнут ни по одному каналу. Это означает, что

$$\overline{M} = \overline{M}_1 \cap \overline{M}_2.$$

Реализация угроз происходит независимо. Значит, события $\overline{M}_1$ и $\overline{M}_2$ также независимы. Поэтому вероятность их пересечения равна произведению их вероятностей:

$$\mathrm{P}\Big(\overline{M}\Big) = \mathrm{P}\Big(\overline{M}_1\Big) \cdot \mathrm{P}\Big(\overline{M}_2\Big).$$

Требуется найти вероятность противоположного события M:

$$\mathrm{P}(M) = 1 - \mathrm{P}\Big(\overline{M}\Big) = 1 - \Big(\big(1 - \mathrm{P}(M_1)\big) \cdot \big(1 - \mathrm{P}(M_2)\big)\Big).$$

Пусть $\mathrm{P}(M_1) = a$ и $\mathrm{P}(M_2) = b$. Искомая вероятность $\mathrm{P}(M) = x$. Рассмотрим эту вероятность как функцию от a и b: $x\,(a,\, b) = 1 - (1 - a)(1 - b)$. Данная функция линейна по каждой из своих переменных. Если увеличить значение a, не меняя b, то значение x увеличится. То же верно для b. Поэтому нижняя оценка вероятности получается из наименьших значений a и b, а верхняя — из наибольших. Найдём эти значения:

$$x_{min} = 1 - (1 - 0,1)(1 - 0,15) = 0,235; \quad x_{max} = 1 - (1 - 0,2)(1 - 0,25) = 0,4.$$

Математический блок. Задание 8.3 (5 баллов).

В системе мониторинга транзакций зафиксировано 2026 кошельков, и любые два кошелька связаны либо прямой транзакцией, либо через цепочку переводов. Кошельки, между которыми был прямой перевод, назовём контрагентами.

Назовём кошелёк рядовым, если число его контрагентов меньше, чем среднее число контрагентов у всех его контрагентов. Если у кошелька контрагентов больше, чем среднее число контрагентов у всех его контрагентов, то такой кошелёк назовём подозрительным хабом.

Могла ли схема взаимодействий сложиться так, что в системе не было ни подозрительных хабов, ни рядовых кошельков? Обязательно обоснуйте свой ответ.

Ответ: да.

Решение. Приведём один из возможных примеров. Будем описывать схему взаимодействий между кошельками при помощи графа: кошельки — его вершины, а транзакции между ними — рёбра.

Для такой схемы подходят так называемые *равномерные* графы — такие, где все вершины имеют одинаковую степень. Например, в полном графе K_{2026} у всех вершин степень равна 2025. В цикле из всех вершин каждая из них имеет степень 2.

У всех вершин в равномерном графе одинаковая степень. Тогда средняя степень всех соседей у всех вершин тоже такая же. Значит, ни одна вершина не является ни рядовой, ни подозрительным хабом.

Математический блок. Задание 8.4 (5 баллов).

В рамках проверки системы бюджетного контроля корпорации были проведены 10 измерений отклонений фактических расходов подразделений от плановых значений (в условных единицах). Результаты измерений представлены в таблице:

Номер измерения	1	2	3	4	5	6	7	8	9	10
Отклонение, у.е.	$-2,2$	$0,4$	$8,7$	$-9,4$	$6,8$	$9,1$	$1,9$	$-3,5$	$5,3$	$-6,1$

Для каждого измерения вычисляется параметр надёжности — модуль его отклонения от среднего арифметического. Измерение считается ненадёжным (подозрительным), если его параметр надёжности отличается от среднего значения параметра надёжности более чем в $1,6$ раза.

Исключите из массива данных измерений ненадёжные. Найдите размах оставшихся измерений.

Ответ: $15,2$.

Решение. Среднее арифметическое измерений равно

$$0,1 \cdot (-2,2 + 0,4 + 8,7 - 9,4 + 6,8 + 9,1 + 1,9 - 3,5 + 5,3 - 6,1) = 1,1.$$

В таблице посчитаем параметры надёжности для каждого измерения.

Номер измерения	1	2	3	4	5	6	7	8	9	10
Значение	$-2,2$	$0,4$	$8,7$	$-9,4$	$6,8$	$9,1$	$1,9$	$-3,5$	$5,3$	$-6,1$
Параметр надёжности	$3,3$	$0,7$	$7,6$	$10,5$	$5,7$	8	$0,8$	$4,6$	$4,2$	$7,2$

Средний параметр надёжности

$$s = 0,1 \cdot (3,3 + 0,7 + 7,6 + 10,5 + 5,7 + 8 + 0,8 + 4,6 + 4,2 + 7,2) = 5,26.$$

Границы интервала в $1,6$ раза от него: $s/1,6 = 3,2875$ и $1,6s = 8,416$.

Подозрительными будем считать измерения, параметр надёжности которых не попадает в промежуток $[3,2875;\ 8,416]$. Это значения с номерами 2, 4 и 7. Исключаем их. Остаются измерения с номерами 1, 2, 3, 5, 6, 8, 9 и 10. Размах — это разность между наибольшим и наименьшим значениями: $9,1 - (-6,1) = 15,2$.

Математический блок. Задание 8.5 (5 баллов).

В системе мониторинга финансовой безопасности за сутки фиксируются сессии клиента в интернет–банке. Каждой сессии начисляется уровень риска по следующим правилам:

1) если вход выполнен с нового устройства, начисляется 3 балла риска;
2) если вход выполнен из нового города, начисляется 2 балла риска;
3) если вход выполнен в ночное время, начисляется 1 балл риска.

Сессия считается подозрительной, если она набрала 5 или 6 баллов риска.

Из отчёта за неделю известно, что:

1) клиент совершил 42 сессии, за которые получил суммарно 80 баллов риска;
2) количество сессий с нулевым числом баллов риска было в 2 раза больше, чем количество подозрительных сессий;
3) количество ночных подозрительных сессий было в 3 раза меньше, чем количество дневных подозрительных сессий.

Найдите максимальное количество подозрительных сессий.

Ответ: 12.

Решение. Сессии, набравшие не менее 5 баллов риска, должны быть с нового устройства и из нового города (иначе баллов риска будет недостаточно). Различие лишь во времени входа. Пусть ночных подозрительных сессий было a, тогда дневных было $3a$. Всего подозрительных сессий $4a$, а «нулевых» в два раза больше, то есть $8a$. Всего сессий не менее чем $a + 3a + 8a = 12a$, а по условию их 42. Значит, $a \leqslant 3$. Поскольку нужно найти максимальное число подозрительных сессий, будем рассматривать наибольшее возможное значение.

Предположим, что $a = 3$. Тогда подозрительные сессии дали $6 \cdot a + 5 \cdot 3a = 63$ балла риска. Осталось ещё 12 сессий и $85 - 66 = 19$ баллов риска. Это возможно, например, если было 7 сессий с 2 баллами риска и 5 сессий с 1 баллом риска.

Получили, что максимально возможное значение $a = 3$. Всего подозрительных сессий при этом 12.

Гуманитарный блок. Задание 8.1.

Прочитайте текст и выполните задания к нему.

(А) Теневой экономикой принято называть хозяйственную деятельность юридических и физических лиц, которая развивается вне государственного учёта и контроля, а потому не отражается в официальной статистике. Как правило, о теневой экономике говорят как о части экономики в целом. Отмечается снижение объёмов теневой экономики за последние годы. По данным исследований, проведённых Национальным институтом системных исследований проблем предпринимательства, масштабы теневой деятельности с 2002 по 2006 годы несколько уменьшились — с 45% до 38% в среднем от оборота фирм.

(Б) Развитие теневой экономики связано, прежде всего, с наличием государственного регулирования. Государственное регулирование предусматривает ряд ограничений, а если есть какие-либо ограничения, обязательно будут их нарушения, особенно если это выгодно для предпринимателей. Высокие налоговые ставки были и остаются основной причиной ухода в тень и сокрытия реальных масштабов деятельности предприятий даже при учёте того фактора, что малые предприятия работают по специальным режимам налогообложения. Система льготного налогообложения обладает серьёзным дефектом, т. к. мешает развитию бизнеса: если оборот малого предприятия растёт, оно может попасть в другие, невыгодные условия налогообложения. Всё это заставляет предпринимателя дробить бизнес, обманывать власть, усложнять менеджмент. Находясь в тени, наладить высокотехнологичное производство невозможно, а лёгкость уклонения от налогов делают более выгодным вложение средств в примитивные виды деятельности. Всё это в итоге тормозит развитие бизнеса. Однако даже при самых минимальных налоговых ставках обязательно найдутся те, кто будет уклоняться от уплаты налогов. Человек всегда стремится получать больше, затрачивая при этом меньше усилий.

(В) С другой стороны, современная теневая экономика возникла не только в результате попыток ограничить свободу рынка, но и в силу природы самих рыночных отношений. Рыночное хозяйство построено на прибыли, на обожествлении дохода. Поэтому отдельные лица часто отбрасывают в сторону долгосрочные общественные интересы ради сиюминутной своекорыстной выгоды. Природу человека нельзя изменить, но человеческое поведение зависит и от окружающей среды, воспитания, образования. Чем больше развиты в обществе этические нормы, которые не приветствуют конфликт с законом, тем менее вероятно такое поведение.

(Г) Во многом уходу в тень способствует внешняя среда — если большинство предприятий используют теневые схемы, то выйти из этого круга какому-то одному предприятию очень не просто. Необходимость ухода в тень продиктована необходимостью «выжить на рынке». Таким образом, предприниматели проводят «вчёрную» часть выплат за аренду помещений, расчёты с поставщиками, по-прежнему широко распространена выплата зарплат в «конверте». Все эти расходы могут быть покрыты только с помощью «теневых средств».

(Д) Следовательно, масштабы теневой деятельности предприятия во многом зависят от внешних факторов, а именно от бизнес–среды и стимулов, создаваемых сотрудниками государственных органов. Для того чтобы вывести малый и средний бизнес из тени, необходимо совершенствовать, прежде всего, правовую систему. Легальная предпринимательская деятельность должна быть более привлекательна и менее рискованна, чем теневая. Особенно важно максимально продумать меры государственного регулирования легальной экономической деятельности.

(По Клямина О.С. Масштабы и причины существования теневой экономики в малом и среднем бизнесе сферы услуг // Сервис в России и за рубежом, 2010)

Вопрос 1.1 (2 балла). Согласно тексту, какая причина является основной для ухода бизнеса в «тень»?

1) Отсутствие спроса на продукцию.
2) Высокие налоговые ставки.
3) Низкая квалификация работников.
4) Избыток государственной поддержки.

Ответ: 2.

Пояснение. В абзаце (Б) текста автор прямо указывает: «*Высокие налоговые ставки были и остаются основной причиной ухода в тень и сокрытия реальных масштабов деятельности предприятий...*» Эта формулировка однозначно определяет высокие налоги как ключевой фактор, что делает вариант 2 единственно верным.

Вопрос 1.2 (3 балла). По мнению автора текста, теневая экономика развивается вне государственного учёта и контроля. Какие риски для государства несёт такая ситуация? Выберите все верные варианты ответа и поясните свой выбор.

1) Снижение налоговых поступлений в бюджет, что ограничивает финансирование социальных программ.
2) Ослабление контроля за экономическими процессами и снижение достоверности официальной статистики.
3) Автоматическое повышение инвестиционной привлекательности страны для иностранного капитала.
4) Снижение эффективности государственных программ поддержки бизнеса из-за искажённых данных о реальной экономике.
5) Упрощение работы правоохранительных органов за счёт меньшего объёма отчётности.
6) Ускорение экономического роста за счёт неучтённой деловой активности.

Ответ: 1, 2, 4.

Пояснение. Почему выбраны варианты 1, 2, 4.

1) Если деятельность не учитывается государством, налоги с неё не уплачиваются или уплачиваются не в полном объёме. Это напрямую ведёт к снижению налоговых поступлений в бюджет, что ограничивает возможности государства финансировать образование, здравоохранение, инфраструктуру.
2) Автор прямо указывает: теневая экономика «*не отражается в официальной статистике*». Это означает, что государство не имеет достоверных данных об объёмах производства, занятости, доходах населения, что ослабляет контроль за экономическими процессами и снижает качество управленческих решений.
4) Если реальные масштабы бизнеса скрыты, государственные программы поддержки (субсидии, гранты, льготные кредиты) могут распределяться неэффективно: помощь получают не те, кто в ней действительно нуждается, или ресурсы распределяются на основе искажённой информации.

Почему не выбраны варианты 3, 5, 6.

3) В тексте нет указаний на то, что теневая экономика повышает инвестиционную привлекательность. Напротив, непрозрачность обычно отпугивает серьёзных инвесторов.
5) Теневая деятельность усложняет, а не упрощает работу правоохранительных органов, так как требует дополнительных ресурсов для выявления нарушений.
6) Автор подчёркивает, что теневая экономика «*тормозит развитие бизнеса*» (абзац Б), а не ускоряет экономический рост.

Гуманитарный блок. Задание 8.2.

Прочитайте текст и выполните задания к нему.

Ученица 9 класса Света (15 лет) нашла в магазине чужую банковскую карту. Карта была с технологией бесконтактной оплаты. Света знала, что владельца карты искать бесполезно, и решила потратить деньги. Она оплатила картой покупку в этом же магазине на сумму 800 рублей, просто приложив карту к терминалу, а затем совершила ещё три покупки в разных местах на общую сумму 3 200 рублей. Всего Света потратила 4 000 рублей. Через неделю к ней домой пришли сотрудники полиции. Света заявила, что не знала, что найденной картой пользоваться нельзя, ведь это не кража — она же не целенаправленно забирала карту у владельца.

Вопрос 2.1 (1 балл). Как квалифицируются действия Светы по расходованию денег с найденной карты?

1) Административное правонарушение (мелкое хищение), так как сумма ущерба не превышает 5 000 рублей, а Свете нет 16 лет.
2) Присвоение находки, которое влечёт только гражданско–правовую ответственность (возврат неосновательного обогащения).
3) Кража, совершённая с банковского счета, независимо от суммы похищенного и от того, как была получена карта (найдена или украдена).
4) Мошенничество, так как Света обманула кассиров, предъявив чужую карту как свою.
5) Грабёж, поскольку оплата проходила открыто в присутствии продавцов.
6) Действия Светы не являются преступлением, так как она не взламывала защиту и не подбирала ПИН–код.

Ответ: 3.

Пояснение. Хищение денежных средств с банковской карты квалифицируется как кража, совершённая с банковского счёта, — п. «г» ч. 3 ст. 158 УК РФ. Это тяжкое преступление. Не имеет значения, была карта украдена, найдена или получена иным незаконным способом. Также не имеет значения способ хищения — через банкомат, оплата покупок в магазине (в том числе бесконтактная оплата) или перевод на другой счёт. Сумма похищенного не влияет на квалификацию (преступление считается оконченным с момента списания денег, даже если сумма незначительная). Варианты 1, 2, 4, 5 и 6 полностью противоречат закону и разъяснениям Верховного Суда РФ.

Вопрос 2.2 (1 балл). С какого возраста наступает ответственность за действия Светы по расходованию денег с найденной карты?

1) С 14 лет.
2) С 16 лет.
3) С 18 лет.
4) Ответственность не наступает, так как действия Светы не являются преступлением.

Ответ: 1.

Пояснение. За преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счёта), уголовная ответственность наступает с 14 лет. Это прямое указание ч. 2 ст. 20 УК РФ, так как данное преступление отнесено к категории тяжких и включено в перечень. Особое внимание: для квалификации не имеет значения, была карта украдена или найдена, а также не имеет значения сумма похищенного.

Вопрос 2.3 (3 балла). Выберите верные утверждения о правовой природе действий Светы и возможных последствиях. Дайте краткое пояснение, почему остальные варианты содержат юридические или финансовые неточности.

1) Использование найденной карты квалифицируется как кража с банковского счёта, поскольку происходит неправомерное обращение чужих денежных средств.
2) Ответственность наступает только при сумме ущерба свыше 5 000 рублей, так как меньшие суммы регулируются КоАП РФ как мелкое хищение.
3) Родители Светы несут гражданскую ответственность за возмещение ущерба, если у подростка нет личного дохода.
4) Если Света добровольно вернёт деньги владельцу до обращения в полицию, уголовное дело не может быть возбуждено в принципе.
5) Найденная карта является «находкой» по смыслу ГК РФ, поэтому её использование влечёт только обязанность передать карту в банк или полицию.
6) Магазин, где была совершена покупка, несёт солидарную ответственность за ущерб, так как терминал не запросил ПИН–код при бесконтактной оплате.

Ответ: 1, 3.

Пояснение. Вариант 2 ошибочен: кража с банковского счёта (п. «г» ч. 3 ст. 158 УК РФ) является уголовным преступлением независимо от суммы.

Вариант 4 неверен: преступление считается оконченным в момент списания средств. Добровольное возмещение может стать основанием для прекращения дела за примирением (ст. 76 УК РФ), но не блокирует возбуждение автоматически.

Вариант 5 отражает бытовое заблуждение: электронные средства платежа не подпадают под правила о находке (ст. 227 ГК РФ) в части права на использование.

Вариант 6 не соответствует практике: риск несанкционированных бесконтактных операций лежит на банке/эквайере и правонарушителе, но не на торговой точке, если терминал исправен.

Гуманитарный блок. Задание 8.3.

Ниже приведены этапы классической мошеннической атаки в интернете, при которой злоумышленники выдают себя за доверенный источник, чтобы «выудить» у жертвы конфиденциальную информацию: логины, пароли, данные банковских карт, персональные данные.

1) Подготовка «наживки»: создание поддельного письма, сайта или сообщения, имитирующего официальный источник (банк, платёжная система, госуслуги). Используются логотипы, похожие доменные имена, официальный стиль общения.
2) Создание «крючка»: в сообщение добавляется эмоциональный триггер — например, срочность, выгода или страх.
3) Атака («подсечка»): жертва переходит по ссылке, вводит данные на поддельной странице или скачивает вредоносное вложение. Злоумышленник получает доступ к информации или устройству.
4) Использование данных: украденная информация используется для несанкционированных транзакций, продажи на чёрном рынке или дальнейших атак.

Вопрос 3.1 (1 балл). Каким термином наиболее точно можно назвать описанный вид интернет–мошенничества?

1) Вишинг.
2) Скимминг.
3) Смишинг.
4) Фишинг.

Ответ: 4.

Пояснение. В тексте описана классическая схема фишинговой атаки.

Фишинг — это вид интернет-мошенничества, при котором злоумышленники, маскируясь под доверенные организации (банки, платёжные системы, государственные органы), пытаются выудить у жертвы конфиденциальную информацию.

Вишинг — это телефонное мошенничество, использующее социальную инженерию для кражи денег или личных данных.

Скимминг — это вид мошенничества, когда злоумышленники крадут данные банковских карт с помощью специальных устройств (скиммеров), установленных на банкоматах или платёжных терминалах.

Смишинг — это вид мошенничества, при котором злоумышленники рассылают фишинговые SMS–сообщения или сообщения в мессенджерах с целью украсть конфиденциальные данные.

Вопрос 3.2 (2 балла). Выберите элементы стратегии защиты, которые минимизируют риск утечки данных жертвы такой атаки.

1) Включить двухфакторную аутентификацию (2FA) для всех финансовых сервисов.
2) Использовать один и тот же сложный пароль для всех сервисов, чтобы не забывать, но регулярно менять его раз в месяц.
3) Регулярно проверять выписки по карте на наличие незнакомых операций, в том числе очень маленьких платежей.
4) Отключить уведомления от банка, чтобы не реагировать на «поддельные», и проверять баланс только вручную.
5) Переходить по ссылкам только из СМС, так как они проходят проверку на безопасность у мобильного оператора.

Ответ: 1, 3.

Пояснение. Вариант 1 верен: двухфакторная идентификация значительно усложняет доступ даже при утечке пароля.

Вариант 3 верен: регулярная проверка выписок по карте позволяет своевременно заметить подозрительные списания.

Вариант 2 ошибочен: повторное использование паролей увеличивает риск повторных утечек при получении доступа к данным одной учётной записи.

Вариант 4 ошибочен: отключение уведомлений уменьшает вероятность своевременно заметить подозрительные списания.

Вариант 5 ошибочен: операторы не проверяют содержание ссылок в СМС–сообщениях.

Вопрос 3.3 (2 балла). Какие психологические приёмы из перечисленных наиболее эффективно заставляют людей терять бдительность? Аргументируйте свой выбор.

1) Использование страха потери («счёт будет заблокирован», «вы потеряете доступ»).
2) Обращение по имени и отчеству, которое совпадает с данными в открытых источниках.
3) Имитация официального стиля: логотип, реквизиты, подпись «Служба безопасности».
4) Указание точного времени дедлайна («через 1 час», «до 18:00»).
5) Предложение «быстрого решения» («нажмите одну кнопку», «введите код из СМС»).
6) Упоминание реальных событий (например, «в связи с обновлением системы безопасности»).

Ответ: 1, 4.

Пояснение. Вариант 1 верен: страх — один из самых сильных триггеров. Когда человек боится потерять деньги или доступ к важному сервису, он склонен действовать импульсивно, не проверяя информацию. Мошенники намеренно создают угрозу, чтобы отключить критическое мышление.

Вариант 4 верен: искусственное ограничение времени лишает жертву возможности спокойно обдумать ситуацию, посоветоваться с близкими или проверить информацию через официальные каналы. Мозг переключается в режим «спасти сейчас», а не «проанализировать».

Вариант 2 неверен: это элемент маскировки, а не эмоционального воздействия. Мошенники собирают имена из соцсетей и утечек, но само по себе обращение по имени не заставляет человека действовать необдуманно.

Вариант 3 неверен: это технический приём подделки, а не психологический триггер. Он работает на доверие к форме, но не создаёт эмоционального давления, которое заставляет действовать «здесь и сейчас».

Варианты 5 и 6 можно отнести как к верным, так и к неверным, наличие данных элементов в ответе не влияет на оценку.

Гуманитарный блок. Задание 8.4.

Прочитайте текст и выполните задания к нему.

Сева и Егор учились в десятом классе и в последнее время всё чаще говорили о деньгах, как будто взрослая жизнь уже стояла где-то совсем рядом. Хотелось многого: купить хорошие наушники, не просить у родителей деньги на каждую мелочь, иметь возможность заказать что-нибудь в интернете без долгих объяснений. После уроков они обычно шли одной и той же дорогой — мимо аптеки, мимо киоска с выпечкой, мимо остановки, где ветер всё время шевелил старые объявления. Иногда они заходили к Егору, ставили чайник и подолгу сидели на кухне, где за окном рано темнело, а на столе рядом с кружками лежали тетради и наскоро брошенные ручки.

Однажды разговор снова зашёл о заработке. Обычные подработки казались им слишком скучными и медленными, а хотелось чего-то более лёгкого, современного, почти не требующего усилий. Егор сказал, что в интернете главное — не столько продавать что-то, сколько создавать у людей ощущение удачной возможности. Сева сначала только усмехнулся, но потом оба открыли телефоны и начали записывать идеи. Постепенно у них сложился план: создать закрытое сообщество, куда можно вступить за небольшую сумму, а потом объяснять новым участникам, что они смогут вернуть свои деньги, если приведут ещё двоих. Тем, в свою очередь, нужно будет сделать то же самое, и процент от взносов пойдёт тем, кто присоединился раньше.

Через несколько дней у них уже была страница с аккуратной обложкой, короткими фразами про рост, развитие и новые возможности и общий чат, который постепенно начал наполняться людьми. Всё выглядело спокойно и даже солидно: сообщения, списки, таблица с именами, переводы, вопросы о том, как подключить следующих. Сева следил за перепиской и отмечал, кто за кем пришёл, а Егор больше занимался тем, как всё подать, чтобы схема казалась понятной и выгодной. В школе при этом ничего не менялось: контрольные шли одна за другой, кто-то перед уроком торопливо списывал домашнее задание, в столовой по-прежнему спорили о еде, а после звонка коридоры снова наполнялись обычным шумом.

Сначала им казалось, что всё складывается удачно. Люди вступали, задавали вопросы, переводили деньги, интересовались, когда можно приглашать новых участников. Телефон у Севы всё чаще вспыхивал от уведомлений, и это придавало происходящему какую-то взрослую серьёзность. Но со временем в чате стали появляться другие сообщения. Кто-то писал, что заплатил, но не понимает, что делать дальше. Кто-то спрашивал, откуда вообще должны появляться деньги, которые обещали в начале. А однажды один из участников добавил в переписку своего отца, и после этого всё изменилось.

На следующий день Егора с родителями вызвали в полицию, и он сразу сообщил об этом Севе по СМС. Тот прочитал сообщение дважды, потом молча положил телефон экраном вниз и посмотрел в окно, за которым начинал капать дождь.

Вопрос 4.1 (2 балла). Приведите термин, наиболее соответствующий явлению, описанному в тексте.

Ответ: Финансовая пирамида.

Пояснение. В тексте описана схема, в которой участники вносят деньги за вход, а затем должны приводить новых людей, чтобы вернуть свои вложения и получить прибыль. Доход в такой системе возникает не за счёт продажи полезного товара или реальной услуги, а в основном за счёт денег следующих участников. Именно это и является главным признаком финансовой пирамиды.

Вопрос 4.2 (3 балла). Опишите в небольшом тексте от 100 до 300 символов, что может привлечь жертв к участию в данной схеме.

Пример ответа: Жертв привлекают обещания сверхдоходов без усилий, иллюзия лёгких денег и давление знакомых. Мошенники играют на жадности и страхе упустить выгоду, маскируя схему под надёжный бизнес.

Гуманитарный блок. Задание 8.5.

Рассмотрите приведённую иллюстрацию и выполните задания к ней.

Вопрос 5.1 (2 балла). Приведите термин, используемый для описания изображённого явления.

Ответ: Дропперство.

Пояснение. На картинке показана конкретная схема прогонки денег через чужие счета/карты/телефоны. Банк России прямо описывает это так: преступники выводят деньги жертв через счета других лиц, а человек, который предоставляет для этого свою карту или счёт, становится дроппером. Именно это и видно на изображении: левая девочка получает «грязные» деньги и передаёт дальше, у второй деньги выглядят уже «чище», а затем уходят ещё дальше. Акцент на роли посредников, через которых прогоняют деньги. Это и есть логика дропперства.

Вопрос 5.2 (1 балл). Выберите статью УК РФ, которая больше всего подходит для описания явления, приведённого на изображении.

Статья 158. Кража
Статья 165. Причинение имущественного ущерба путём обмана или злоупотребления доверием
Статья 172. Незаконная банковская деятельность
Статья 172.2. Организация деятельности по привлечению денежных средств и (или) иного имущества
Статья 179. Принуждение к совершению сделки или к отказу от её совершения
Статья 186. Изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг
Статья 187. Неправомерный оборот средств платежей
Статья 198. Уклонение физического лица от уплаты налогов, сборов и (или) физического лица — плательщика страховых взносов от уплаты страховых взносов
Статья 204. Коммерческий подкуп

Ответ: Статья 187. Неправомерный оборот средств платежей.

Пояснение. Из предложенных вариантов лучше всего подходит статья 187 УК РФ. После изменений 2025 года она прямо охватывает передачу электронного средства платежа и (или) доступа к нему другому лицу для осуществления неправомерных операций. Именно это и составляет суть дропперства: человек предоставляет свою карту, счёт, онлайн–банк или доступ к ним, чтобы через них прогоняли чужие незаконные деньги.

Вопрос 5.3 (2 балла). Приятель предложил вам принять участие в похожей схеме. Напишите в небольшом тексте от 100 до 300 символов, как бы вы ему ответили и почему.

Пример ответа: Я в таком участвовать не буду. Это дропперство, уголовное преступление. Дропперов сажают в тюрьму и блокируют счета. Никакая комиссия не стоит свободы и испорченной жизни. Лучше поискать законный способ заработать.

Кейс. При домашнем написании одной очень интересной и ответственной Олимпиады некоторые недобросовестные участники решили воспользоваться ИИ, загрузили задачи в подходящие платформы от Алисы до DeepSeekMath, получили от них решения и выдали их за свои.

Жюри Олимпиады тоже умеет пользоваться искусственным интеллектом, в частности, для распознавания работ, написанных при помощи искусственного интеллекта. Проверка идет про трём признакам. Не будем вдаваться в детали и назовём их признаки А, Б и В.

В случае, если работа содержит признак А работы ИИ, автор дисквалифицируется (работа снимается с проверки, а участник выбывает из конкурса) независимо от прочих обстоятельств. Обнаружение же признаков Б и В требует экспертизы. В случае, если экспертиза подтверждает работу ИИ, автор также дисквалифицируется.

Исследование показало, что часть участников, пользующихся ИИ, пытаются перерабатывать полученные от ИИ тексты, после чего признаки А и Б иногда исчезают или почти исчезают. При этом были получены следующие верные количественные оценки.

1) Признак А проявляется в 100% работ, выполненных ИИ, но доля недобросовестных участников, умеющих избавляться от данного признака, равна 30%.
2) Признак Б проявляется в 90% работ, сделанных с участием ИИ, и экспертиза признаёт их несомненно недобросовестными с вероятностью $0,6$.
3) Признак В проявляется в 60% работ, сделанных при помощи ИИ, и экспертиза признаёт их недобросовестными с вероятностью $0,8$.
4) Признаки А, Б и В присутствуют во всех текстах ИИ независимо друг от друга.

Проверка Олимпиады выявила, что признак А работы ИИ присутствует в 9 000 из 15 000 сданных участниками работ.

Задание 1 (5 баллов). Считая все имеющиеся оценки точными, найдите долю участников, которые писали работу честно, не прибегая к использованию ИИ.

Задание 2 (5 баллов). Считая все имеющиеся оценки точными, найдите долю дисквалифицированных среди недобросовестных участников.

Задание 3 (5 баллов). Считая все имеющиеся оценки точными, найдите долю дисквалифицированных среди тех недобросовестных участников, кто избавился от признака А работы ИИ.

Ответ: 1) $\frac{1}{7}$; **2)** прибл. $0,928$; **3)** прибл. $0,761$.

Решение. Пусть доля добросовестных участников равна p. Тогда доля недобросовестных участников равна $1-p$. Из них 30% избавились от признака А, а 70% не умеют этого делать. Их доля от общего количества равна $0,7(1-p)$. Эти работы и были выявлены во время проверки. Её результаты показывают: доля недобросовестных участников, не избавившихся от признака А, равна $9000/15000 = 0,6$. Получаем уравнение $0,7(1-p) = 0,6$, откуда $p = 1/7$.

Доля участников с какими-то параметрами совпадает с вероятностью для случайно выбранного участника иметь эти параметры. Поэтому для удобства перейдём от долей к вероятностям.

Рассмотрим участников, использовавших в своих работах ИИ. Признак А не выявляется с вероятностью $0,3$. Признак Б выявляется с вероятностью $0,9 \cdot 0,6 = 0,54$, а не выявляется — с вероятностью $1-0,54 = 0,46$. Аналогично с признаком В — вероятность его невыявления $1-0,6 \cdot 0,8 = 0,52$. Участник не дисквалифицирован, если в его работе не выявлен ни один из признаков. Их выявление происходит независимо. Поэтому вероятность невыявления ни одного из признаков равна произведению вероятностей невыявления для каждого из них: $0,3 \cdot 0,46 \cdot 0,52 = 0,07176$. Значит, вероятность дисквалификации для использовавших ИИ равна $1-0,07176 = 0,92824 \approx 0,928$.

Рассмотрим только участников, избавившихся от признака А. Для них дисквалификация происходит по признакам Б и В. Аналогично предыдущему пункту вероятность невыявления ни одного из признаков Б и В равна $0,46 \cdot 0,52 = 0,2392$. Значит, вероятность дисквалификации для избавившихся от признака А равна $1-0,2392 = 0,7608 \approx 0,761$.

Критерии оценивания.

Проверка олимпиадных работ осуществляется по заданиям. В каждом задании комиссия проверяет ответ, а также правильность, самостоятельность и полноту решения.

Ответ без объяснения не оценивается.

В случае неверного ответа за задание выставляется 0 баллов.

В случае, если решение задания выполнено с нарушением п. 29 Порядка проведения олимпиад школьников, за задание выставляется 0 баллов.

Математический блок и Кейс.

- Приведены верный ответ и полное обоснованное решение задачи: максимальный балл.
- Баллы могут быть снижены за арифметические ошибки или неполноту объяснений.

Гуманитарный блок.

- Приведён полностью верный ответ (выбраны все верные варианты ответа и ни одного лишнего): максимальный балл.
- В заданиях 1.2 и 2.3
  - ▶ за каждый выбранный верный вариант ответа начисляется 1 балл;
  - ▶ за каждый выбранный неверный вариант ответа снимается 1 балл.
- В задании 3.3
  - ▶ за каждый выбранный верный вариант ответа начисляется 1 балл;
  - ▶ за каждый выбранный неверный вариант ответа снимается 1 балл;
  - ▶ выбор элементов 5 и 6 не влияет на оценку, их можно как указать, так и пропустить.

Математический блок. Задание 9.1 (5 баллов).

Старшеклассник Петя, желая быстро заработать и не зная об уголовной ответственности за неправомерный оборот электронного средства платежа, отозвался на объявление о поиске сотрудников для «тестирования нагрузки на платёжную систему» и согласился стать дропом. По указанию, поступившему в чате, он зарегистрировал один электронный кошелёк для получения средств и далее каждые 12 минут из каждого уже созданного кошелька он отправлял по 3 ссылки, ведущие на регистрацию новых кошельков, и активировал их.

Система финансового мониторинга инициирует проверку, как только количество кошельков, зарегистрированных с одного IP–адреса, достигает 65. Через какое время (в минутах) с момента регистрации первого электронного кошелька Петя будет обнаружен?

Примечание: все регистрации происходят мгновенно, а все кошельки автоматически привязываются к Петиному IP–адресу.

Ответ: 48 минут.

Решение. За одну итерацию из каждого созданного кошелька отправляются три ссылки, по которым активируются новые кошельки. Обозначим X_k количество зарегистрированных кошельков через k таких итераций. По условию $X_0 = 1$. Каждый раз количество увеличивается в 4 раза: $X_k = 4X_{k-1}$. Найдём несколько последовательных значений:

$$X_0 = 1;\ X_1 = 4 \cdot 1 = 4;\ X_2 = 4 \cdot 4 = 16;\ X_3 = 4 \cdot 16 = 64;\ X_4 = 4 \cdot 64 = 256.$$

После четырёх итераций число зарегистрированных Петей кошельков становится больше 65. Одна итерация занимает 12 минут. Значит, Петя будет обнаружен через $4 \cdot 12 = 48$ минут.

Математический блок. Задание 9.2 (5 баллов).

Служба финансовой безопасности крупной корпорации анализирует риски потери средств при проведении электронных транзакций. Система защиты имеет три независимых канала уязвимости (А, Б и В). Экспертная оценка определила вероятности возникновения финансовых потерь по каждому из каналов следующим образом.

- В связи с уязвимостью внутреннего сервера (канал А): от $0,1$ до $0,2$.
- В связи с риском фишинговой атаки на сотрудников (канал Б): от $0,1$ до $0,2$.
- В связи с возможным сбоем платёжного шлюза (канал В): от $0,1$ до $0,15$.

Реализация угроз по разным каналам происходит независимо. На основании этих данных оцените снизу и сверху вероятность того, что у корпорации возникнут финансовые потери.

Ответ: $[0,271;\ 0,456]$.

Решение. Обозначим события M «*возникнут финансовые потери*», M_1 «*финансовые потери возникнут в связи с каналом А*», M_2 «*потери возникнут в связи с каналом Б*» и M_3 «*потери возникнут в связи с каналом В*». Потерь не будет, если они не возникнут ни по одному каналу. Это означает, что

$$\overline{M} = \overline{M}_1 \cap \overline{M}_2 \cap \overline{M}_3.$$

Реализация угроз происходит независимо. Значит, события $\overline{M}_1$, $\overline{M}_2$ и $\overline{M}_3$ также независимы. Поэтому вероятность их пересечения равна произведению их вероятностей:

$$\mathrm{P}\Big(\overline{M}\Big) = \mathrm{P}\Big(\overline{M}_1\Big) \cdot \mathrm{P}\Big(\overline{M}_2\Big) \cdot \mathrm{P}\Big(\overline{M}_3\Big).$$

Требуется найти вероятность противоположного события M:

$$\mathrm{P}(M) = 1 - \mathrm{P}\Big(\overline{M}\Big) = 1 - \Big(\big(1 - \mathrm{P}(M_1)\big) \cdot \big(1 - \mathrm{P}(M_2)\big) \cdot \big(1 - \mathrm{P}(M_3)\big)\Big).$$

Пусть $\mathrm{P}(M_1) = a$, $\mathrm{P}(M_2) = b$, $\mathrm{P}(M_3) = c$. Искомая вероятность $\mathrm{P}(M) = x$. Рассмотрим эту вероятность как функцию от a, b и c: $x\,(a,\, b,\, c) = 1 - (1-a)(1-b)(1-c)$. Данная функция линейна по каждой из своих переменных. Если увеличить значение a, не меняя остальные, то значение x увеличится. То же верно для b и c. Поэтому нижняя оценка вероятности получается из наименьших значений a, b и c, а верхняя — из наибольших. Найдём эти значения:

$$x_{min} = 1 - (1-0,1)(1-0,1)(1-0,1) = 0,271; \quad x_{max} = 1 - (1-0,2)(1-0,2)(1-0,15) = 0,456.$$

Математический блок. Задание 9.3 (5 баллов).

В системе мониторинга транзакций зафиксировано 2026 кошельков, и любые два кошелька связаны либо прямой транзакцией, либо через цепочку переводов. Кошельки, между которыми был прямой перевод, назовём контрагентами.

Назовём кошелёк рядовым, если число его контрагентов меньше, чем среднее число контрагентов у всех его контрагентов. Если у кошелька контрагентов больше, чем среднее число контрагентов у всех его контрагентов, то такой кошелёк назовём подозрительным хабом.

Могла ли схема взаимодействий сложиться так, что в системе было больше рядовых кошельков, чем остальных? Обязательно обоснуйте свой ответ.

Ответ: да.

Решение. Приведём один из возможных примеров. Будем описывать схему взаимодействий между кошельками при помощи графа: кошельки — его вершины, а транзакции между ними — рёбра.

Возьмём одну вершину и назовём её H. Оставшиеся вершины составят множество R. Вершину H соединим со всеми остальными вершинами (такой граф иногда называют «звезда»). У вершины H все соседи имеют степень 1. Средняя степень её соседей равна $1 < 2025$, значит, вершина H — хаб. У каждой вершины из R всего один сосед со степенью $2025 > 1$, значит, эта вершина рядовая. Получаем, что рядовых больше, чем остальных вершин.

Математический блок. Задание 9.4 (5 баллов).

В рамках проверки системы бюджетного контроля корпорации были проведены 10 измерений отклонений фактических расходов подразделений от плановых значений (в условных единицах). Результаты измерений представлены в таблице:

Номер измерения	1	2	3	4	5	6	7	8	9	10
Отклонение, у.е.	$-8,8$	$-2,3$	$8,7$	$-7,2$	$-4,5$	$9,6$	$-5,7$	$3,8$	$-0,6$	1

Для каждого измерения вычисляется параметр надёжности — модуль его отклонения от среднего арифметического. Измерение считается ненадёжным (подозрительным), если его параметр надёжности отличается от стандартного отклонения более чем на 30%.

Исключите из массива данных измерений ненадёжные. Найдите медиану оставшихся измерений.

Ответ: $-5,7$.

Решение. Среднее арифметическое измерений равно

$$0,1 \cdot (-8,8 - 2,3 + 8,7 - 7,2 - 4,5 + 9,6 - 5,7 + 3,8 - 0,6 + 1) = -0,6.$$

В таблице посчитаем параметры надёжности для каждого измерения.

Номер измерения	1	2	3	4	5	6	7	8	9	10
Значение	$-8,8$	$-2,3$	$8,7$	$-7,2$	$-4,5$	$9,6$	$-5,7$	$3,8$	$-0,6$	1
Параметр надёжности	$8,2$	$1,7$	$9,3$	$6,6$	$3,9$	$10,2$	$5,1$	$4,4$	0	$1,6$

Дисперсия измерений

$$0,1 \cdot \left(8,2^2 + 1,7^2 + 9,3^2 + 6,6^2 + 3,9^2 + 10,2^2 + 5,1^2 + 4,4^2 + 0^2 + 1,6^2\right) \approx 36,736.$$

Найдём стандартное отклонение: $s \approx \sqrt{36,736} \approx 6,06$. Границы интервала $\pm 30\%$ от него: $0,7s \approx 4,24$ и $1,3s \approx 7,88$.

Подозрительными будем считать измерения, параметр надёжности которых не попадает в промежуток $[4,24;\ 7,88]$. Это значения с номерами 1, 2, 3, 5, 6, 9 и 10. Исключаем их. Остаются измерения с номерами 4, 7 и 8. Для удобства нахождения медианы упорядочим их по возрастанию: $-7,2;\ -5,7;\ 3,8$. Медианой будет второе число в ряду, то есть $-5,7$.

Математический блок. Задание 9.5 (5 баллов).

В системе мониторинга финансовой безопасности за сутки фиксируются сессии клиента в интернет–банке. Каждой сессии начисляется уровень риска по следующим правилам:

1) если вход выполнен с нового устройства, начисляется 3 балла риска;
2) если вход выполнен из нового города, начисляется 2 балла риска;
3) если вход выполнен в ночное время, начисляется 1 балл риска.

Сессия считается подозрительной, если она набрала 5 или 6 баллов риска.

Из отчёта за неделю известно, что:

1) клиент совершил 48 сессий, за которые получил суммарно 85 баллов риска;
2) количество сессий с нулевым числом баллов риска было в 2 раза больше, чем количество подозрительных сессий;
3) количество ночных подозрительных сессий было в 3 раза меньше, чем количество дневных подозрительных сессий.

Найдите максимальное количество подозрительных сессий.

Ответ: 12.

Решение. Сессии, набравшие не менее 5 баллов риска, должны быть с нового устройства и из нового города (иначе баллов риска будет недостаточно). Различие лишь во времени входа. Пусть ночных подозрительных сессий было a, тогда дневных было $3a$. Всего подозрительных сессий $4a$, а «нулевых» в два раза больше, то есть $8a$. Всего сессий не менее чем $a + 3a + 8a = 12a$, а по условию их 48. Значит, $a \leqslant 4$. Поскольку нужно найти максимальное число подозрительных сессий, будем рассматривать наибольшее возможное значение.

Предположим, что $a = 4$. Тогда подозрительные сессии дали $6 \cdot a + 5 \cdot 3a = 84$ балла риска. Остался ещё $85 - 84 = 1$ балл риска, но сессий больше не осталось. Противоречие.

Рассмотрим $a = 3$. Тогда подозрительные сессии принесли $6 \cdot a + 5 \cdot 3a = 63$ балла риска. Осталось ещё 12 сессий и $85 - 63 = 22$ балла риска. Это возможно, например, если было 10 сессий с 2 баллами риска и 2 сессии с 1 баллом риска.

Получили, что максимально возможное значение $a = 3$. Всего подозрительных сессий при этом 12.

Гуманитарный блок. Задание 9.1.

Прочитайте текст и выполните задания к нему.

(А) Теневой экономикой принято называть хозяйственную деятельность юридических и физических лиц, которая развивается вне государственного учёта и контроля, а потому не отражается в официальной статистике. Как правило, о теневой экономике говорят как о части экономики в целом. Отмечается снижение объёмов теневой экономики за последние годы. По данным исследований, проведённых Национальным институтом системных исследований проблем предпринимательства, масштабы теневой деятельности с 2002 по 2006 годы несколько уменьшились — с 45% до 38% в среднем от оборота фирм.

(Б) Развитие теневой экономики связано, прежде всего, с наличием государственного регулирования. Государственное регулирование предусматривает ряд ограничений, а если есть какие-либо ограничения, обязательно будут их нарушения, особенно если это выгодно для предпринимателей. Высокие налоговые ставки были и остаются основной причиной ухода в тень и сокрытия реальных масштабов деятельности предприятий даже при учёте того фактора, что малые предприятия работают по специальным режимам налогообложения. Система льготного налогообложения обладает серьёзным дефектом, т. к. мешает развитию бизнеса: если оборот малого предприятия растёт, оно может попасть в другие, невыгодные условия налогообложения. Всё это заставляет предпринимателя дробить бизнес, обманывать власть, усложнять менеджмент. Находясь в тени, наладить высокотехнологичное производство невозможно, а лёгкость уклонения от налогов делают более выгодным вложение средств в примитивные виды деятельности. Всё это в итоге тормозит развитие бизнеса. Однако даже при самых минимальных налоговых ставках обязательно найдутся те, кто будет уклоняться от уплаты налогов. Человек всегда стремится получать больше, затрачивая при этом меньше усилий.

(В) С другой стороны, современная теневая экономика возникла не только в результате попыток ограничить свободу рынка, но и в силу природы самих рыночных отношений. Рыночное хозяйство построено на прибыли, на обожествлении дохода. Поэтому отдельные лица часто отбрасывают в сторону долгосрочные общественные интересы ради сиюминутной своекорыстной выгоды. Природу человека нельзя изменить, но человеческое поведение зависит и от окружающей среды, воспитания, образования. Чем больше развиты в обществе этические нормы, которые не приветствуют конфликт с законом, тем менее вероятно такое поведение.

(Г) Во многом уходу в тень способствует внешняя среда — если большинство предприятий используют теневые схемы, то выйти из этого круга какому-то одному предприятию очень не просто. Необходимость ухода в тень продиктована необходимостью «выжить на рынке». Таким образом, предприниматели проводят «вчёрную» часть выплат за аренду помещений, расчёты с поставщиками, по-прежнему широко распространена выплата зарплат в «конверте». Все эти расходы могут быть покрыты только с помощью «теневых средств».

(Д) Следовательно, масштабы теневой деятельности предприятия во многом зависят от внешних факторов, а именно от бизнес–среды и стимулов, создаваемых сотрудниками государственных органов. Для того чтобы вывести малый и средний бизнес из тени, необходимо совершенствовать, прежде всего, правовую систему. Легальная предпринимательская деятельность должна быть более привлекательна и менее рискованна, чем теневая. Особенно важно максимально продумать меры государственного регулирования легальной экономической деятельности.

(По Клямина О.С. Масштабы и причины существования теневой экономики в малом и среднем бизнесе сферы услуг // Сервис в России и за рубежом, 2010)

Вопрос 1.1 (2 балла). Какой вывод делает автор текста о мерах по выводу бизнеса из тени?

1) Необходимо полностью отменить налогообложение для малого бизнеса.
2) Достаточно усилить контроль и штрафы за нарушения.
3) Легальная предпринимательская деятельность должна стать более привлекательной и менее рискованной, чем теневая.
4) Следует запретить малым предприятиям расширяться.

Ответ: 3.

Пояснение. В заключительном абзаце (Д) автор формулирует главный вывод: «*Легальная предпринимательская деятельность должна быть более привлекательна и менее рискованна, чем теневая*». Эта фраза дословно совпадает с вариантом 3, что делает его правильным. Автор подчёркивает: решение — не в запретах, а в создании экономических стимулов для легальной работы.

Вопрос 1.2 (3 балла). По мнению автора текста, нахождение бизнеса в «тени» имеет негативные последствия для предпринимателей и экономики. Какие из перечисленных утверждений подтверждаются текстом? Выберите все верные варианты ответа и поясните свой выбор.

1) Невозможность наладить высокотехнологичное производство в теневом секторе.
2) Сдвиг инвестиционных предпочтений в сторону примитивных видов деятельности из–за лёгкости уклонения от налогов.
3) Ускорение роста компаний за счёт отсутствия бюрократических процедур.
4) Торможение развития бизнеса, связанное с необходимостью дробить предприятия и усложнять менеджмент.
5) Повышение конкурентоспособности на международном рынке благодаря снижению налоговых издержек.
6) Упрощение процедуры привлечения квалифицированных кадров.

Ответ: 1, 2, 4.

Пояснение. Почему выбраны варианты 1, 2, 4.

1) Автор прямо пишет: «*Находясь в тени, наладить высокотехнологичное производство невозможно*». Это связано с тем, что теневая деятельность требует постоянной конспирации, ограничивает доступ к легальным кредитам, инвестициям и современным технологиям.
2) В тексте указано: «*лёгкость уклонения от налогов делают более выгодным вложение средств в примитивные виды деятельности*». То есть предпринимателю выгоднее вкладываться в простые, быстродоходные схемы, чем в долгосрочные инновационные проекты.
4) Автор подчёркивает: «*Всё это в итоге тормозит развитие бизнеса*», а также отмечает, что предприниматель вынужден «*дробить бизнес, обманывать власть, усложнять менеджмент*». Это создаёт дополнительные издержки и снижает эффективность управления.

Почему не выбраны варианты 3, 5, 6.

3) В тексте нет утверждений об ускорении роста компаний в тени. Напротив, автор говорит о торможении развития.
5) Текст не упоминает о повышении международной конкурентоспособности. Теневые компании, как правило, не могут выходить на легальные международные рынки.
6) Напротив, «теневые» предприятия сталкиваются с ограничениями в доступе к банковским кредитам и государственным программам поддержки, так как не могут подтвердить свои доходы официально.

Гуманитарный блок. Задание 9.2.

Ученица 9 класса Света (15 лет) нашла в магазине чужую банковскую карту. Карта была с технологией бесконтактной оплаты. Света знала, что владельца карты искать бесполезно, и решила потратить деньги. Она оплатила картой покупку в этом же магазине на сумму 800 рублей, просто приложив карту к терминалу, а затем совершила ещё три покупки в разных местах на общую сумму 3 200 рублей. Всего Света потратила 4 000 рублей. Через неделю к ней домой пришли сотрудники полиции. Света заявила, что не знала, что найденной картой пользоваться нельзя, ведь это не кража — она же не целенаправленно забирала карту у владельца.

Вопрос 2.1 (1 балл). Как квалифицируются действия Светы по расходованию денег с найденной карты?

1) Административное правонарушение (мелкое хищение), так как сумма ущерба не превышает 5 000 рублей, а Свете нет 16 лет.
2) Присвоение находки, которое влечёт только гражданско–правовую ответственность (возврат неосновательного обогащения).
3) Кража, совершённая с банковского счета, независимо от суммы похищенного и от того, как была получена карта (найдена или украдена).
4) Мошенничество, так как Света обманула кассиров, предъявив чужую карту как свою.
5) Грабёж, поскольку оплата проходила открыто в присутствии продавцов.
6) Действия Светы не являются преступлением, так как она не взламывала защиту и не подбирала ПИН–код.

Ответ: 3.

Пояснение. Хищение денежных средств с банковской карты квалифицируется как кража, совершённая с банковского счёта, — п. «г» ч. 3 ст. 158 УК РФ. Это тяжкое преступление. Не имеет значения, была карта украдена, найдена или получена иным незаконным способом. Также не имеет значения способ хищения — через банкомат, оплата покупок в магазине (в том числе бесконтактная оплата) или перевод на другой счёт. Сумма похищенного не влияет на квалификацию (преступление считается оконченным с момента списания денег, даже если сумма незначительная). Варианты 1, 2, 4, 5 и 6 полностью противоречат закону и разъяснениям Верховного Суда РФ.

Вопрос 2.2 (1 балл). С какого возраста наступает ответственность за действия Светы по расходованию денег с найденной карты?

1) С 14 лет.
2) С 16 лет.
3) С 18 лет.
4) Ответственность не наступает, так как действия Светы не являются преступлением.

Ответ: 1.

Пояснение. За преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счёта), уголовная ответственность наступает с 14 лет. Это прямое указание ч. 2 ст. 20 УК РФ, так как данное преступление отнесено к категории тяжких и включено в перечень. Особое внимание: для квалификации не имеет значения, была карта украдена или найдена, а также не имеет значения сумма похищенного.

Вопрос 2.3 (3 балла). Выберите верные утверждения о классификации ответственности и процессуальных особенностях дела. Аргументируйте выбор, опираясь на нормы права и финансовую практику.

1) Действия Светы подпадают под п. «г» ч. 3 ст. 158 УК РФ, поскольку хищение совершено с использованием платёжного средства, привязанного к банковскому счёту.
2) Уголовная ответственность за данное деяние наступает с 16 лет, так как ст. 158 УК РФ не входит в перечень преступлений с пониженным возрастным порогом.
3) Незнание закона является обстоятельством, исключающим преступность деяния по УК РФ.
4) Если ущерб будет возмещён в полном объёме, суд может освободить Свету от уголовной ответственности в связи с деятельным раскаянием или примирением с потерпевшим.
5) Поскольку оплата была бесконтактной и не требовала ПИН–кода, состав преступления отсутствует — это техническая ошибка эквайринга.
6) Комиссии за перевод средств, проценты по кредиту или штрафы банка (если карта была кредитной) не включаются в размер ущерба при квалификации преступления.

Ответ: 1, 4, 6.

Пояснение. Вариант 2 ошибочен: ст. 20 УК РФ прямо устанавливает возраст ответственности за кражу (включая кражу с банковского счёта) с 14 лет.

Вариант 3 противоречит базовому принципу права: незнание закона не освобождает от ответственности.

Вариант 5 игнорирует субъективную сторону: умысел на безвозмездное обращение чужих средств присутствует независимо от способа авторизации.

Вариант 6 соответствует разъяснениям Пленума ВС РФ: при квалификации учитывается фактически изъятая сумма; банковские комиссии и проценты регулируются гражданско–правовыми отношениями между держателем карты и банком.

Гуманитарный блок. Задание 9.3.

Ниже приведены этапы классической мошеннической атаки в интернете, при которой злоумышленники выдают себя за доверенный источник, чтобы «выудить» у жертвы конфиденциальную информацию: логины, пароли, данные банковских карт, персональные данные.

1) Подготовка «наживки»: создание поддельного письма, сайта или сообщения, имитирующего официальный источник (банк, платёжная система, госуслуги). Используются логотипы, похожие доменные имена, официальный стиль общения.
2) Создание «крючка»: в сообщение добавляется эмоциональный триггер — например, срочность, выгода или страх.
3) Атака («подсечка»): жертва переходит по ссылке, вводит данные на поддельной странице или скачивает вредоносное вложение. Злоумышленник получает доступ к информации или устройству.
4) Использование данных: украденная информация используется для несанкционированных транзакций, продажи на чёрном рынке или дальнейших атак.

Вопрос 3.1 (1 балл). Каким термином наиболее точно можно назвать описанный вид интернет–мошенничества?

1) Вишинг.
2) Скимминг.
3) Смишинг.
4) Фишинг.

Ответ: 4.

Пояснение. В тексте описана классическая схема фишинговой атаки.

Фишинг — это вид интернет-мошенничества, при котором злоумышленники, маскируясь под доверенные организации (банки, платёжные системы, государственные органы), пытаются выудить у жертвы конфиденциальную информацию.

Вишинг — это телефонное мошенничество, использующее социальную инженерию для кражи денег или личных данных.

Скимминг — это вид мошенничества, когда злоумышленники крадут данные банковских карт с помощью специальных устройств (скиммеров), установленных на банкоматах или платёжных терминалах.

Смишинг — это вид мошенничества, при котором злоумышленники рассылают фишинговые SMS–сообщения или сообщения в мессенджерах с целью украсть конфиденциальные данные.

Вопрос 3.2 (2 балла). Выберите элементы стратегии защиты, которые минимизируют риск утечки данных жертвы такой атаки.

1) Включить двухфакторную аутентификацию (2FA) для всех финансовых сервисов.
2) Использовать один и тот же сложный пароль для всех сервисов, чтобы не забывать, но регулярно менять его раз в месяц.
3) Регулярно проверять выписки по карте на наличие незнакомых операций, в том числе очень маленьких платежей.
4) Отключить уведомления от банка, чтобы не реагировать на «поддельные», и проверять баланс только вручную.
5) Переходить по ссылкам только из СМС, так как они проходят проверку на безопасность у мобильного оператора.

Ответ: 1, 3.

Пояснение. Вариант 1 верен: двухфакторная идентификация значительно усложняет доступ даже при утечке пароля.

Вариант 3 верен: регулярная проверка выписок по карте позволяет своевременно заметить подозрительные списания.

Вариант 2 ошибочен: повторное использование паролей увеличивает риск повторных утечек при получении доступа к данным одной учётной записи.

Вариант 4 ошибочен: отключение уведомлений уменьшает вероятность своевременно заметить подозрительные списания.

Вариант 5 ошибочен: операторы не проверяют содержание ссылок в СМС–сообщениях.

Вопрос 3.3 (2 балла). Какие психологические приёмы из перечисленных наиболее эффективно заставляют людей терять бдительность? Аргументируйте свой выбор.

1) Использование страха потери («счёт будет заблокирован», «вы потеряете доступ»).
2) Обращение по имени и отчеству, которое совпадает с данными в открытых источниках.
3) Имитация официального стиля: логотип, реквизиты, подпись «Служба безопасности».
4) Указание точного времени дедлайна («через 1 час», «до 18:00»).
5) Предложение «быстрого решения» («нажмите одну кнопку», «введите код из СМС»).
6) Упоминание реальных событий (например, «в связи с обновлением системы безопасности»).

Ответ: 1, 4.

Пояснение. Вариант 1 верен: страх — один из самых сильных триггеров. Когда человек боится потерять деньги или доступ к важному сервису, он склонен действовать импульсивно, не проверяя информацию. Мошенники намеренно создают угрозу, чтобы отключить критическое мышление.

Вариант 4 верен: искусственное ограничение времени лишает жертву возможности спокойно обдумать ситуацию, посоветоваться с близкими или проверить информацию через официальные каналы. Мозг переключается в режим «спасти сейчас», а не «проанализировать».

Вариант 2 неверен: это элемент маскировки, а не эмоционального воздействия. Мошенники собирают имена из соцсетей и утечек, но само по себе обращение по имени не заставляет человека действовать необдуманно.

Вариант 3 неверен: это технический приём подделки, а не психологический триггер. Он работает на доверие к форме, но не создаёт эмоционального давления, которое заставляет действовать «здесь и сейчас».

Варианты 5 и 6 можно отнести как к верным, так и к неверным, наличие данных элементов в ответе не влияет на оценку.

Гуманитарный блок. Задание 9.4.

Прочитайте текст и выполните задания к нему.

Сева и Егор учились в десятом классе и в последнее время всё чаще говорили о деньгах, как будто взрослая жизнь уже стояла где-то совсем рядом. Хотелось многого: купить хорошие наушники, не просить у родителей деньги на каждую мелочь, иметь возможность заказать что-нибудь в интернете без долгих объяснений. После уроков они обычно шли одной и той же дорогой — мимо аптеки, мимо киоска с выпечкой, мимо остановки, где ветер всё время шевелил старые объявления. Иногда они заходили к Егору, ставили чайник и подолгу сидели на кухне, где за окном рано темнело, а на столе рядом с кружками лежали тетради и наскоро брошенные ручки.

Однажды разговор снова зашёл о заработке. Обычные подработки казались им слишком скучными и медленными, а хотелось чего-то более лёгкого, современного, почти не требующего усилий. Егор сказал, что в интернете главное — не столько продавать что-то, сколько создавать у людей ощущение удачной возможности. Сева сначала только усмехнулся, но потом оба открыли телефоны и начали записывать идеи. Постепенно у них сложился план: создать закрытое сообщество, куда можно вступить за небольшую сумму, а потом объяснять новым участникам, что они смогут вернуть свои деньги, если приведут ещё двоих. Тем, в свою очередь, нужно будет сделать то же самое, и процент от взносов пойдёт тем, кто присоединился раньше.

Через несколько дней у них уже была страница с аккуратной обложкой, короткими фразами про рост, развитие и новые возможности и общий чат, который постепенно начал наполняться людьми. Всё выглядело спокойно и даже солидно: сообщения, списки, таблица с именами, переводы, вопросы о том, как подключить следующих. Сева следил за перепиской и отмечал, кто за кем пришёл, а Егор больше занимался тем, как всё подать, чтобы схема казалась понятной и выгодной. В школе при этом ничего не менялось: контрольные шли одна за другой, кто-то перед уроком торопливо списывал домашнее задание, в столовой по-прежнему спорили о еде, а после звонка коридоры снова наполнялись обычным шумом.

Сначала им казалось, что всё складывается удачно. Люди вступали, задавали вопросы, переводили деньги, интересовались, когда можно приглашать новых участников. Телефон у Севы всё чаще вспыхивал от уведомлений, и это придавало происходящему какую-то взрослую серьёзность. Но со временем в чате стали появляться другие сообщения. Кто-то писал, что заплатил, но не понимает, что делать дальше. Кто-то спрашивал, откуда вообще должны появляться деньги, которые обещали в начале. А однажды один из участников добавил в переписку своего отца, и после этого всё изменилось.

На следующий день Егора с родителями вызвали в полицию, и он сразу сообщил об этом Севе по СМС. Тот прочитал сообщение дважды, потом молча положил телефон экраном вниз и посмотрел в окно, за которым начинал капать дождь.

Вопрос 4.1 (2 балла). Приведите термин, наиболее соответствующий явлению, описанному в тексте.

Ответ: Финансовая пирамида.

Пояснение. В тексте описана схема, в которой участники вносят деньги за вход, а затем должны приводить новых людей, чтобы вернуть свои вложения и получить прибыль. Доход в такой системе возникает не за счёт продажи полезного товара или реальной услуги, а в основном за счёт денег следующих участников. Именно это и является главным признаком финансовой пирамиды.

Вопрос 4.2 (3 балла). Опишите в небольшом тексте от 100 до 300 символов, что может привлечь жертв к участию в данной схеме.

Пример ответа: Жертв привлекают обещания сверхдоходов без усилий, иллюзия лёгких денег и давление знакомых. Мошенники играют на жадности и страхе упустить выгоду, маскируя схему под надёжный бизнес.

Гуманитарный блок. Задание 9.5.

Рассмотрите приведённую иллюстрацию и выполните задания к ней.

Вопрос 5.1 (2 балла). Приведите термин, используемый для описания изображённого явления.

Ответ: Дропперство.

Пояснение. На картинке показана конкретная схема прогонки денег через чужие счета/карты/телефоны. Банк России прямо описывает это так: преступники выводят деньги жертв через счета других лиц, а человек, который предоставляет для этого свою карту или счёт, становится дроппером. Именно это и видно на изображении: левая девочка получает «грязные» деньги и передаёт дальше, у второй деньги выглядят уже «чище», а затем уходят ещё дальше. Акцент на роли посредников, через которых прогоняют деньги. Это и есть логика дропперства.

Вопрос 5.2 (1 балл). Выберите статью УК РФ, которая больше всего подходит для описания явления, приведённого на изображении.

Статья 158. Кража
Статья 165. Причинение имущественного ущерба путём обмана или злоупотребления доверием
Статья 172. Незаконная банковская деятельность
Статья 172.2. Организация деятельности по привлечению денежных средств и (или) иного имущества
Статья 179. Принуждение к совершению сделки или к отказу от её совершения
Статья 186. Изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг
Статья 187. Неправомерный оборот средств платежей
Статья 198. Уклонение физического лица от уплаты налогов, сборов и (или) физического лица — плательщика страховых взносов от уплаты страховых взносов
Статья 204. Коммерческий подкуп

Ответ: Статья 187. Неправомерный оборот средств платежей.

Пояснение. Из предложенных вариантов лучше всего подходит статья 187 УК РФ. После изменений 2025 года она прямо охватывает передачу электронного средства платежа и (или) доступа к нему другому лицу для осуществления неправомерных операций. Именно это и составляет суть дропперства: человек предоставляет свою карту, счёт, онлайн–банк или доступ к ним, чтобы через них прогоняли чужие незаконные деньги.

Вопрос 5.3 (2 балла). Приятель предложил вам принять участие в похожей схеме. Напишите в небольшом тексте от 100 до 300 символов, как бы вы ему ответили и почему.

Пример ответа: Я в таком участвовать не буду. Это дропперство, уголовное преступление. Дропперов сажают в тюрьму и блокируют счета. Никакая комиссия не стоит свободы и испорченной жизни. Лучше поискать законный способ заработать.

Кейс. При домашнем написании одной очень интересной и ответственной Олимпиады некоторые недобросовестные участники решили воспользоваться ИИ, загрузили задачи в подходящие платформы от Алисы до DeepSeekMath, получили от них решения и выдали их за свои.

Жюри Олимпиады тоже умеет пользоваться искусственным интеллектом, в частности, для распознавания работ, написанных при помощи искусственного интеллекта. Проверка идет про трём признакам. Не будем вдаваться в детали и назовём их признаки А, Б и В.

В случае, если работа содержит признак А работы ИИ, автор дисквалифицируется (работа снимается с проверки, а участник выбывает из конкурса) независимо от прочих обстоятельств. Обнаружение же признаков Б и В требует экспертизы. В случае, если экспертиза подтверждает работу ИИ, автор также дисквалифицируется.

Исследование показало, что часть участников, пользующихся ИИ, пытаются перерабатывать полученные от ИИ тексты, после чего признаки А и Б иногда исчезают или почти исчезают. При этом были получены следующие верные количественные оценки.

1) Признак А проявляется в 100% работ, выполненных ИИ, но доля недобросовестных участников, умеющих избавляться от данного признака, равна 30%.
2) Признак Б проявляется в 90% работ, сделанных с участием ИИ, и экспертиза признаёт их несомненно недобросовестными с вероятностью $0,6$.
3) Признак В проявляется в 60% работ, сделанных при помощи ИИ, и экспертиза признаёт их недобросовестными с вероятностью $0,8$.
4) Признаки А, Б и В присутствуют во всех текстах ИИ независимо друг от друга.

Проверка Олимпиады выявила, что признак А работы ИИ присутствует в 9 000 из 15 000 сданных участниками работ.

Задание 1 (5 баллов). Считая все имеющиеся оценки точными, найдите долю участников, которые писали работу честно, не прибегая к использованию ИИ.

Задание 2 (5 баллов). Считая все имеющиеся оценки точными, найдите долю дисквалифицированных среди недобросовестных участников.

Задание 3 (5 баллов). Считая все имеющиеся оценки точными, найдите долю дисквалифицированных среди тех недобросовестных участников, кто избавился от признака А работы ИИ.

Ответ: 1) $\frac{1}{7}$; **2)** прибл. $0,928$; **3)** прибл. $0,761$.

Решение. Пусть доля добросовестных участников равна p. Тогда доля недобросовестных участников равна $1-p$. Из них 30% избавились от признака А, а 70% не умеют этого делать. Их доля от общего количества равна $0,7(1-p)$. Эти работы и были выявлены во время проверки. Её результаты показывают: доля недобросовестных участников, не избавившихся от признака А, равна $9000/15000 = 0,6$. Получаем уравнение $0,7(1-p) = 0,6$, откуда $p = 1/7$.

Доля участников с какими-то параметрами совпадает с вероятностью для случайно выбранного участника иметь эти параметры. Поэтому для удобства перейдём от долей к вероятностям.

Рассмотрим участников, использовавших в своих работах ИИ. Признак А не выявляется с вероятностью $0,3$. Признак Б выявляется с вероятностью $0,9 \cdot 0,6 = 0,54$, а не выявляется — с вероятностью $1-0,54 = 0,46$. Аналогично с признаком В — вероятность его невыявления $1-0,6 \cdot 0,8 = 0,52$. Участник не дисквалифицирован, если в его работе не выявлен ни один из признаков. Их выявление происходит независимо. Поэтому вероятность невыявления ни одного из признаков равна произведению вероятностей невыявления для каждого из них: $0,3 \cdot 0,46 \cdot 0,52 = 0,07176$. Значит, вероятность дисквалификации для использовавших ИИ равна $1-0,07176 = 0,92824 \approx 0,928$.

Рассмотрим только участников, избавившихся от признака А. Для них дисквалификация происходит по признакам Б и В. Аналогично предыдущему пункту вероятность невыявления ни одного из признаков Б и В равна $0,46 \cdot 0,52 = 0,2392$. Значит, вероятность дисквалификации для избавившихся от признака А равна $1-0,2392 = 0,7608 \approx 0,761$.

Критерии оценивания.

Проверка олимпиадных работ осуществляется по заданиям. В каждом задании комиссия проверяет ответ, а также правильность, самостоятельность и полноту решения.

Ответ без объяснения не оценивается.

В случае неверного ответа за задание выставляется 0 баллов.

В случае, если решение задания выполнено с нарушением п. 29 Порядка проведения олимпиад школьников, за задание выставляется 0 баллов.

Математический блок и Кейс.

- Приведены верный ответ и полное обоснованное решение задачи: максимальный балл.
- Баллы могут быть снижены за арифметические ошибки или неполноту объяснений.

Гуманитарный блок.

- Приведён полностью верный ответ (выбраны все верные варианты ответа и ни одного лишнего): максимальный балл.
- В заданиях 1.2 и 2.3
  - ► за каждый выбранный верный вариант ответа начисляется 1 балл;
  - ► за каждый выбранный неверный вариант ответа снимается 1 балл.
- В задании 3.3
  - ► за каждый выбранный верный вариант ответа начисляется 1 балл;
  - ► за каждый выбранный неверный вариант ответа снимается 1 балл;
  - ► выбор элементов 5 и 6 не влияет на оценку, их можно как указать, так и пропустить.

Математический блок. Задание 10.1 (5 баллов).

Старшеклассник Петя, желая быстро заработать и не зная об уголовной ответственности за неправомерный оборот электронного средства платежа, отозвался на объявление о поиске сотрудников для «тестирования нагрузки на платёжную систему» и согласился стать дропом. По указанию, поступившему в чате, он зарегистрировал два электронных кошелька для получения средств и далее каждые 10 минут из каждого уже созданного кошелька он отправлял по 3 ссылки, ведущие на регистрацию новых кошельков, и активировал их.

Система финансового мониторинга инициирует проверку, как только количество кошельков, зарегистрированных с одного IP–адреса, достигает 75. Через какое время (в минутах) с момента регистрации первого электронного кошелька Петя будет обнаружен?

Примечание: все регистрации происходят мгновенно, а все кошельки автоматически привязываются к Петиному IP–адресу.

Ответ: 30 минут.

Решение. За одну итерацию из каждого созданного кошелька отправляются три ссылки, по которым активируются новые кошельки. Обозначим X_k количество зарегистрированных кошельков через k таких итераций. По условию $X_0 = 2$. Каждый раз количество увеличивается в 4 раза: $X_k = 4X_{k-1}$. Найдём несколько последовательных значений:

$$X_0 = 2;\ X_1 = 4 \cdot 2 = 8;\ X_2 = 4 \cdot 8 = 32;\ X_3 = 4 \cdot 32 = 128.$$

После трёх итераций число зарегистрированных Петей кошельков становится больше 75. Одна итерация занимает 10 минут. Значит, Петя будет обнаружен через $3 \cdot 10 = 30$ минут.

Математический блок. Задание 10.2 (5 баллов).

Служба финансовой безопасности крупной корпорации анализирует риски потери средств при проведении электронных транзакций. Система защиты имеет три независимых канала уязвимости (А, Б и В). Экспертная оценка определила вероятности возникновения финансовых потерь по каждому из каналов следующим образом.

- В связи с уязвимостью внутреннего сервера (канал А): от $0,164$ до $0,2$.
- В связи с риском фишинговой атаки на сотрудников (канал Б): от $0,15$ до $0,2$.
- В связи с возможным сбоем платёжного шлюза (канал В): от $0,11$ до $0,17$.

Реализация угроз по разным каналам происходит независимо. На основании этих данных оцените снизу и сверху вероятность того, что у корпорации возникнут финансовые потери. Округлите результат до 3 знаков после запятой.

Ответ: $[0,368;\ 0,469]$.

Решение. Обозначим события M «*возникнут финансовые потери*», M_1 «*финансовые потери возникнут в связи с каналом А*», M_2 «*потери возникнут в связи с каналом Б*» и M_3 «*потери возникнут в связи с каналом В*». Потерь не будет, если они не возникнут ни по одному каналу. Это означает, что

$$\overline{M} = \overline{M}_1 \cap \overline{M}_2 \cap \overline{M}_3.$$

Реализация угроз происходит независимо. Значит, события $\overline{M}_1$, $\overline{M}_2$ и $\overline{M}_3$ также независимы. Поэтому вероятность их пересечения равна произведению их вероятностей:

$$\mathrm{P}\Big(\overline{M}\Big) = \mathrm{P}\Big(\overline{M}_1\Big) \cdot \mathrm{P}\Big(\overline{M}_2\Big) \cdot \mathrm{P}\Big(\overline{M}_3\Big).$$

Требуется найти вероятность противоположного события M:

$$\mathrm{P}(M) = 1 - \mathrm{P}\Big(\overline{M}\Big) = 1 - \Big(\big(1 - \mathrm{P}(M_1)\big) \cdot \big(1 - \mathrm{P}(M_2)\big) \cdot \big(1 - \mathrm{P}(M_3)\big)\Big).$$

Пусть $\mathrm{P}(M_1) = a$, $\mathrm{P}(M_2) = b$, $\mathrm{P}(M_3) = c$. Искомая вероятность $\mathrm{P}(M) = x$. Рассмотрим эту вероятность как функцию от a, b и c: $x\,(a,\, b,\, c) = 1 - (1-a)(1-b)(1-c)$. Данная функция линейна по каждой из своих переменных. Если увеличить значение a, не меняя остальные, то значение x увеличится. То же верно для b и c. Поэтому нижняя оценка вероятности получается из наименьших значений a, b и c, а верхняя — из наибольших. Найдём эти значения:

$$x_{min} = 1 - (1 - 0,164)(1 - 0,15)(1 - 0,11) \approx 0,368; \quad x_{max} = 1 - (1 - 0,2)(1 - 0,2)(1 - 0,17) \approx 0,469.$$

Математический блок. Задание 10.3 (5 баллов).

В системе мониторинга транзакций зафиксировано 2026 кошельков, и любые два кошелька связаны либо прямой транзакцией, либо через цепочку переводов. Кошельки, между которыми был прямой перевод, назовём контрагентами.

Назовём кошелёк рядовым, если число его контрагентов меньше, чем среднее число контрагентов у всех его контрагентов. Если у кошелька контрагентов больше, чем среднее число контрагентов у всех его контрагентов, то такой кошелёк назовём подозрительным хабом.

Могла ли схема взаимодействий сложиться так, что в системе было больше подозрительных хабов, чем остальных? Обязательно обоснуйте свой ответ.

Ответ: да.

Решение. Приведём один из возможных примеров. Будем описывать схему взаимодействий между кошельками при помощи графа: кошельки — его вершины, а транзакции между ними — рёбра.

Возьмём 1500 вершин и назовём их множество H. Оставшиеся 526 вершин составят множество R. Каждую вершину из H соединим со всеми остальными из H и со всеми вершинами из R. У каждой вершины из H всего 1499 соседей со степенью 2025 (остальные «хабы») и 526 соседей со степенью 1500 («рядовые»). Значит, средняя степень соседей равна

$$\frac{1499 \cdot 2025 + 526 \cdot 1500}{2025} \approx 1888,6 < 2025.$$

Для каждой вершины из R все её соседи — из H, поэтому их средняя степень равна $2025 > 1500$. Это доказывает, что в построенной схеме все вершины из H — хабы, а остальные — рядовые. При этом хабов больше, чем остальных вершин.

Математический блок. Задание 10.4 (5 баллов).

В рамках проверки системы бюджетного контроля корпорации были проведены 10 измерений отклонений фактических расходов подразделений от плановых значений (в условных единицах). Результаты измерений представлены в таблице:

Номер измерения	1	2	3	4	5	6	7	8	9	10
Отклонение, у.е.	$-6,7$	-4	$1,9$	$-5,9$	$-7,5$	9	$-8,6$	$4,6$	$1,4$	$-0,2$

Для каждого измерения вычисляется параметр надёжности — модуль его отклонения от среднего арифметического. Измерение считается ненадёжным (подозрительным), если его параметр надёжности отличается от стандартного отклонения более чем на 20%.

Исключите из массива данных измерений ненадёжные. Найдите среднее арифметическое оставшихся измерений.

Ответ: $-3,2$.

Решение. Среднее арифметическое измерений равно

$$0,1 \cdot (-6,7 - 4 + 1,9 - 5,9 - 7,5 + 9 - 8,6 + 4,6 + 1,4 - 0,2) = -1,6.$$

В таблице посчитаем параметры надёжности для каждого измерения.

Номер измерения	1	2	3	4	5	6	7	8	9	10
Значение	$-6,7$	-4	$1,9$	$-5,9$	$-7,5$	9	$-8,6$	$4,6$	$1,4$	$-0,2$
Параметр надёжности	$5,1$	$2,4$	$3,5$	$4,3$	$5,9$	$10,6$	7	$6,2$	3	$1,4$

Дисперсия измерений

$$0,1 \cdot \left(5,1^2 + 2,4^2 + 3,5^2 + 4,3^2 + 5,9^2 + 10,6^2 + 7^2 + 6,2^2 + 3^2 + 1,4^2\right) \approx 30,808.$$

Найдём стандартное отклонение: $s \approx \sqrt{30,808} \approx 5,55$. Находим границы интервала для подозрительных измерений $\pm 20\%$ от s: $0,8s \approx 4,44$ и $1,2s \approx 6,66$.

Подозрительными будем считать измерения, параметр надёжности которых не попадает в промежуток $[4,44;\ 6,66]$. Это значения с номерами 2, 3, 4, 6, 7, 9 и 10. Исключаем их. Остаются измерения с номерами 1, 5 и 8. Их среднее арифметическое

$$\frac{1}{3}\left(-6,7 + (-7,5) + 4,6\right) = -3,2.$$

Математический блок. Задание 10.5 (5 баллов).

В системе мониторинга финансовой безопасности за сутки фиксируются сессии клиента в интернет–банке. Каждой сессии начисляется уровень риска по следующим правилам:

1) если вход выполнен с нового устройства, начисляется 3 балла риска;
2) если вход выполнен из нового города, начисляется 2 балла риска;
3) если вход выполнен в ночное время, начисляется 1 балл риска.

Сессия считается подозрительной, если она набрала 5 или 6 баллов риска.

Из отчёта за неделю известно, что:

1) клиент совершил 50 сессий, за которые получил суммарно 93 балла риска;
2) количество сессий с нулевым числом баллов риска было в 2 раза больше, чем количество подозрительных сессий;
3) количество ночных подозрительных сессий было в 3 раза меньше, чем количество дневных подозрительных сессий.

Найдите максимальное количество подозрительных сессий.

Ответ: 12.

Решение. Сессии, набравшие не менее 5 баллов риска, должны быть с нового устройства и из нового города (иначе баллов риска будет недостаточно). Различие лишь во времени входа. Пусть ночных подозрительных сессий было a, тогда дневных было $3a$. Всего подозрительных сессий $4a$, а «нулевых» в два раза больше, то есть $8a$. Всего сессий не менее чем $a + 3a + 8a = 12a$, а по условию их 50. Значит, $a \leqslant 4$. Поскольку нужно найти максимальное число подозрительных сессий, будем рассматривать наибольшее возможное значение.

Предположим, что $a = 4$. Тогда подозрительные сессии дали $6 \cdot a + 5 \cdot 3a = 84$ балла риска. Осталось ещё 2 сессии и $93 - 84 = 9$ баллов риска. Оставшиеся сессии не подозрительные, значит, у каждой из них не более 4 баллов риска. Набрать оставшимися двумя сессиями оставшиеся 9 баллов риска невозможно. Противоречие.

Рассмотрим $a = 3$. Тогда подозрительные сессии принесли $6 \cdot a + 5 \cdot 3a = 63$ балла риска. Осталось ещё 14 сессий и $93 - 63 = 30$ баллов риска. Это возможно, например, если было 2 сессии с 3 баллами риска и 12 сессий с 2 баллами риска.

Получили, что максимально возможное значение $a = 3$. Всего подозрительных сессий при этом 12.

Гуманитарный блок. Задание 10.1.

Прочитайте текст и выполните задания к нему.

(А) Теневой экономикой принято называть хозяйственную деятельность юридических и физических лиц, которая развивается вне государственного учёта и контроля, а потому не отражается в официальной статистике. Как правило, о теневой экономике говорят как о части экономики в целом. Отмечается снижение объёмов теневой экономики за последние годы. По данным исследований, проведённых Национальным институтом системных исследований проблем предпринимательства, масштабы теневой деятельности с 2002 по 2006 годы несколько уменьшились — с 45% до 38% в среднем от оборота фирм.

(Б) Развитие теневой экономики связано, прежде всего, с наличием государственного регулирования. Государственное регулирование предусматривает ряд ограничений, а если есть какие-либо ограничения, обязательно будут их нарушения, особенно если это выгодно для предпринимателей. Высокие налоговые ставки были и остаются основной причиной ухода в тень и сокрытия реальных масштабов деятельности предприятий даже при учёте того фактора, что малые предприятия работают по специальным режимам налогообложения. Система льготного налогообложения обладает серьёзным дефектом, т. к. мешает развитию бизнеса: если оборот малого предприятия растёт, оно может попасть в другие, невыгодные условия налогообложения. Всё это заставляет предпринимателя дробить бизнес, обманывать власть, усложнять менеджмент. Находясь в тени, наладить высокотехнологичное производство невозможно, а лёгкость уклонения от налогов делают более выгодным вложение средств в примитивные виды деятельности. Всё это в итоге тормозит развитие бизнеса. Однако даже при самых минимальных налоговых ставках обязательно найдутся те, кто будет уклоняться от уплаты налогов. Человек всегда стремится получать больше, затрачивая при этом меньше усилий.

(В) С другой стороны, современная теневая экономика возникла не только в результате попыток ограничить свободу рынка, но и в силу природы самих рыночных отношений. Рыночное хозяйство построено на прибыли, на обожествлении дохода. Поэтому отдельные лица часто отбрасывают в сторону долгосрочные общественные интересы ради сиюминутной своекорыстной выгоды. Природу человека нельзя изменить, но человеческое поведение зависит и от окружающей среды, воспитания, образования. Чем больше развиты в обществе этические нормы, которые не приветствуют конфликт с законом, тем менее вероятно такое поведение.

(Г) Во многом уходу в тень способствует внешняя среда — если большинство предприятий используют теневые схемы, то выйти из этого круга какому-то одному предприятию очень не просто. Необходимость ухода в тень продиктована необходимостью «выжить на рынке». Таким образом, предприниматели проводят «вчёрную» часть выплат за аренду помещений, расчёты с поставщиками, по-прежнему широко распространена выплата зарплат в «конверте». Все эти расходы могут быть покрыты только с помощью «теневых средств».

(Д) Следовательно, масштабы теневой деятельности предприятия во многом зависят от внешних факторов, а именно от бизнес–среды и стимулов, создаваемых сотрудниками государственных органов. Для того чтобы вывести малый и средний бизнес из тени, необходимо совершенствовать, прежде всего, правовую систему. Легальная предпринимательская деятельность должна быть более привлекательна и менее рискованна, чем теневая. Особенно важно максимально продумать меры государственного регулирования легальной экономической деятельности.

(По Клямина О.С. Масштабы и причины существования теневой экономики в малом и среднем бизнесе сферы услуг // Сервис в России и за рубежом, 2010)

Вопрос 1.1 (2 балла). Проанализируйте аргументацию автора. Какое из перечисленных утверждений наиболее точно отражает системный подход к проблеме теневой экономики, представленной в тексте?

1) Теневая экономика — это исключительно результат низкой правовой культуры предпринимателей, поэтому решение лежит только в сфере воспитания и образования.
2) Теневая экономика возникает из-за сочетания факторов: государственного регулирования, природы рыночных отношений и внешней бизнес–среды; поэтому для её сокращения нужны комплексные меры, включая совершенствование правовой системы.
3) Теневая экономика — неизбежное зло рыночной системы, и любые попытки государства повлиять на неё только ухудшают ситуацию.
4) Проблема теневой экономики решается автоматически по мере роста ВВП, поэтому государственное вмешательство не требуется.

Ответ: 2.

Пояснение. Автор последовательно раскрывает множество взаимосвязанных причин теневой экономики.

Государственное регулирование и налоги: абзац (Б). «*Развитие теневой экономики связано, прежде всего, с наличием государственного регулирования... Высокие налоговые ставки...*»

Природа рыночных отношений: абзац (В). «*...в силу природы самих рыночных отношений. Рыночное хозяйство построено на прибыли...*»

Внешняя бизнес–среда: абзац (Г). «*Если большинство предприятий используют теневые схемы, то выйти из этого круга... очень не просто*»

Вопрос 1.2 (3 балла). По мнению автора текста, масштабы теневой деятельности зависят от комплекса факторов: государственного регулирования, природы рыночных отношений, этических норм и внешней бизнес–среды. Какие меры, согласно тексту, могут способствовать выводу бизнеса из тени? Выберите все верные варианты ответа и поясните свой выбор.

1) Совершенствование правовой системы, чтобы легальная деятельность стала менее рискованной
2) Создание стимулов через государственные органы, которые поощряют прозрачную и честную деятельность
3) Полная отмена государственного регулирования рыночных отношений
4) Усиление карательных мер без изменения экономических условий для бизнеса
5) Повышение привлекательности легального бизнеса через продуманное налоговое регулирование
6) Обязательное дробление всех предприятий для упрощения государственного контроля

Ответ: 1, 2, 5.

Пояснение. Почему выбраны варианты 1, 2, 5.

1) «*Совершенствовать, прежде всего, правовую систему*» — это прямая цитата из текста. Укрепление правовых гарантий снижает риски легального бизнеса и повышает доверие предпринимателей к государству.
2) Автор указывает, что масштабы теневой деятельности зависят от «*стимулов, создаваемых сотрудниками государственных органов*». Это означает, что госорганы должны не только контролировать, но и поощрять прозрачную деятельность (например, через упрощение процедур, поддержку экспорта, информационное сопровождение).
5) Фраза «*легальная предпринимательская деятельность должна быть более привлекательна*» подразумевает, в том числе, продуманное налоговое регулирование: справедливые ставки, понятные правила, отсутствие «ловушек» при росте бизнеса.

Почему не выбраны варианты 3, 4, 6.

3) Автор не предлагает отменять государственное регулирование. Напротив, он говорит о необходимости его «максимально продумать», то есть сделать более качественным, а не устранить.
4) Усиление исключительно карательных мер без изменения экономических условий противоречит системному подходу автора: если легальная деятельность остаётся рискованной и невыгодной, бизнес будет уходить в тень, несмотря на штрафы.
6) Автор критикует вынужденное дробление бизнеса как негативное последствие несовершенства налоговой системы, а не предлагает делать его обязательным.

Гуманитарный блок. Задание 10.2.

Ученица 9 класса Света (15 лет) нашла в магазине чужую банковскую карту. Карта была с технологией бесконтактной оплаты. Света знала, что владельца карты искать бесполезно, и решила потратить деньги. Она оплатила картой покупку в этом же магазине на сумму 800 рублей, просто приложив карту к терминалу, а затем совершила ещё три покупки в разных местах на общую сумму 3 200 рублей. Всего Света потратила 4 000 рублей. Через неделю к ней домой пришли сотрудники полиции. Света заявила, что не знала, что найденной картой пользоваться нельзя, ведь это не кража — она же не целенаправленно забирала карту у владельца.

Вопрос 2.1 (1 балл). Как квалифицируются действия Светы по расходованию денег с найденной карты?

1) Административное правонарушение (мелкое хищение), так как сумма ущерба не превышает 5 000 рублей, а Свете нет 16 лет.
2) Присвоение находки, которое влечёт только гражданско–правовую ответственность (возврат неосновательного обогащения).
3) Кража, совершённая с банковского счета, независимо от суммы похищенного и от того, как была получена карта (найдена или украдена).
4) Мошенничество, так как Света обманула кассиров, предъявив чужую карту как свою.
5) Грабёж, поскольку оплата проходила открыто в присутствии продавцов.
6) Действия Светы не являются преступлением, так как она не взламывала защиту и не подбирала ПИН–код.

Ответ: 3.

Пояснение. Хищение денежных средств с банковской карты квалифицируется как кража, совершённая с банковского счёта, — п. «г» ч. 3 ст. 158 УК РФ. Это тяжкое преступление. Не имеет значения, была карта украдена, найдена или получена иным незаконным способом. Также не имеет значения способ хищения — через банкомат, оплата покупок в магазине (в том числе бесконтактная оплата) или перевод на другой счёт. Сумма похищенного не влияет на квалификацию (преступление считается оконченным с момента списания денег, даже если сумма незначительная). Варианты 1, 2, 4, 5 и 6 полностью противоречат закону и разъяснениям Верховного Суда РФ.

Вопрос 2.2 (1 балл). С какого возраста наступает ответственность за действия Светы по расходованию денег с найденной карты?

1) С 14 лет.
2) С 16 лет.
3) С 18 лет.
4) Ответственность не наступает, так как действия Светы не являются преступлением.

Ответ: 1.

Пояснение. За преступление, предусмотренное п. «г» ч. 3 ст. 158 УК РФ (кража с банковского счёта), уголовная ответственность наступает с 14 лет. Это прямое указание ч. 2 ст. 20 УК РФ, так как данное преступление отнесено к категории тяжких и включено в перечень. Особое внимание: для квалификации не имеет значения, была карта украдена или найдена, а также не имеет значения сумма похищенного.

Вопрос 2.3 (3 балла). Выберите верные утверждения, отражающие комплексную правовую и финансовую квалификацию ситуации. Аргументируйте выбор, опираясь на нормы права и финансовую практику.

1) Квалификация по п. «г» ч. 3 ст. 158 УК РФ применяется независимо от суммы похищенного, так как объектом преступления выступает банковский счёт.
2) Света может быть привлечена к административной ответственности по ст. 7.27 КоАП РФ за мелкое хищение, если суд признает отсутствие умысла на хищение крупных сумм.
3) Родители Светы не несут ответственность по возмещению ущерба, если докажут, что не могли контролировать её действия.
4) Банк обязан вернуть владельцу карты сумму несанкционированных операций, если клиент своевременно сообщил об утере, но это не освобождает Свету от уголовной ответственности.
5) Если владелец карты не застраховал счёт от мошенничества, он не может требовать возмещения ущерба ни от банка, ни от правонарушителя.
6) Суд может назначить принудительные меры воспитательного воздействия вместо наказания, если учтёт возраст, отсутствие судимостей и полное возмещение ущерба.

Ответ: 1, 4, 6.

Пояснение. Вариант 1 верен: п. «г» ч. 3 ст. 158 УК РФ — специальный состав: хищение с банковского счёта является уголовным преступлением независимо от суммы.

Вариант 2 ошибочен: нельзя привлекать одновременно по УК РФ и КоАП РФ за одно деяние. При наличии состава преступления применяется только уголовная ответственность.

Вариант 3 ошибочен: ответственность родителей по ст. 1073–1074 ГК РФ носит прямой, а не субсидиарный характер и не зависит от того, могли ли они контролировать ребёнка.

Вариант 4 верен: по ФЗ–161 банк обязан возместить клиенту сумму несанкционированной операции (при своевременном уведомлении), но это не отменяет уголовную ответственность правонарушителя.

Вариант 5 ошибочен: право на возмещение ущерба закреплено законом (ГК РФ, ФЗ–161), а не договором страхования. Отсутствие страховки не лишает потерпевшего права на компенсацию.

Вариант 6 верен: ст. 90 УК РФ позволяет суду заменить наказание принудительными мерами воспитательного воздействия при учёте возраста, раскаяния и возмещения вреда.

Гуманитарный блок. Задание 10.3.

Ниже приведены этапы классической мошеннической атаки в интернете, при которой злоумышленники выдают себя за доверенный источник, чтобы «выудить» у жертвы конфиденциальную информацию: логины, пароли, данные банковских карт, персональные данные.

1) Подготовка «наживки»: создание поддельного письма, сайта или сообщения, имитирующего официальный источник (банк, платёжная система, госуслуги). Используются логотипы, похожие доменные имена, официальный стиль общения.
2) Создание «крючка»: в сообщение добавляется эмоциональный триггер — например, срочность, выгода или страх.
3) Атака («подсечка»): жертва переходит по ссылке, вводит данные на поддельной странице или скачивает вредоносное вложение. Злоумышленник получает доступ к информации или устройству.
4) Использование данных: украденная информация используется для несанкционированных транзакций, продажи на чёрном рынке или дальнейших атак.

Вопрос 3.1 (1 балл). Каким термином наиболее точно можно назвать описанный вид интернет–мошенничества?

1) Вишинг.
2) Скимминг.
3) Смишинг.
4) Фишинг.

Ответ: 4.

Пояснение. В тексте описана классическая схема фишинговой атаки.

Фишинг — это вид интернет-мошенничества, при котором злоумышленники, маскируясь под доверенные организации (банки, платёжные системы, государственные органы), пытаются выудить у жертвы конфиденциальную информацию.

Вишинг — это телефонное мошенничество, использующее социальную инженерию для кражи денег или личных данных.

Скимминг — это вид мошенничества, когда злоумышленники крадут данные банковских карт с помощью специальных устройств (скиммеров), установленных на банкоматах или платёжных терминалах.

Смишинг — это вид мошенничества, при котором злоумышленники рассылают фишинговые SMS–сообщения или сообщения в мессенджерах с целью украсть конфиденциальные данные.

Вопрос 3.2 (2 балла). Выберите элементы стратегии защиты, которые минимизируют риск утечки данных жертвы такой атаки.

1) Включить двухфакторную аутентификацию (2FA) для всех финансовых сервисов.
2) Использовать один и тот же сложный пароль для всех сервисов, чтобы не забывать, но регулярно менять его раз в месяц.
3) Регулярно проверять выписки по карте на наличие незнакомых операций, в том числе очень маленьких платежей.
4) Отключить уведомления от банка, чтобы не реагировать на «поддельные», и проверять баланс только вручную.
5) Переходить по ссылкам только из СМС, так как они проходят проверку на безопасность у мобильного оператора.

Ответ: 1, 3.

Пояснение. Вариант 1 верен: двухфакторная идентификация значительно усложняет доступ даже при утечке пароля.

Вариант 3 верен: регулярная проверка выписок по карте позволяет своевременно заметить подозрительные списания.

Вариант 2 ошибочен: повторное использование паролей увеличивает риск повторных утечек при получении доступа к данным одной учётной записи.

Вариант 4 ошибочен: отключение уведомлений уменьшает вероятность своевременно заметить подозрительные списания.

Вариант 5 ошибочен: операторы не проверяют содержание ссылок в СМС–сообщениях.

Вопрос 3.3 (2 балла). Какие психологические приёмы из перечисленных наиболее эффективно заставляют людей терять бдительность? Аргументируйте свой выбор.

1) Использование страха потери («счёт будет заблокирован», «вы потеряете доступ»).
2) Обращение по имени и отчеству, которое совпадает с данными в открытых источниках.
3) Имитация официального стиля: логотип, реквизиты, подпись «Служба безопасности».
4) Указание точного времени дедлайна («через 1 час», «до 18:00»).
5) Предложение «быстрого решения» («нажмите одну кнопку», «введите код из СМС»).
6) Упоминание реальных событий (например, «в связи с обновлением системы безопасности»).

Ответ: 1, 4.

Пояснение. Вариант 1 верен: страх — один из самых сильных триггеров. Когда человек боится потерять деньги или доступ к важному сервису, он склонен действовать импульсивно, не проверяя информацию. Мошенники намеренно создают угрозу, чтобы отключить критическое мышление.

Вариант 4 верен: искусственное ограничение времени лишает жертву возможности спокойно обдумать ситуацию, посоветоваться с близкими или проверить информацию через официальные каналы. Мозг переключается в режим «спасти сейчас», а не «проанализировать».

Вариант 2 неверен: это элемент маскировки, а не эмоционального воздействия. Мошенники собирают имена из соцсетей и утечек, но само по себе обращение по имени не заставляет человека действовать необдуманно.

Вариант 3 неверен: это технический приём подделки, а не психологический триггер. Он работает на доверие к форме, но не создаёт эмоционального давления, заставляющего действовать «здесь и сейчас».

Варианты 5 и 6 можно отнести как к верным, так и к неверным, наличие данных элементов в ответе не влияет на оценку.

Гуманитарный блок. Задание 10.4.

Прочитайте текст и выполните задания к нему.

Сева и Егор учились в десятом классе и в последнее время всё чаще говорили о деньгах, как будто взрослая жизнь уже стояла где-то совсем рядом. Хотелось многого: купить хорошие наушники, не просить у родителей деньги на каждую мелочь, иметь возможность заказать что-нибудь в интернете без долгих объяснений. После уроков они обычно шли одной и той же дорогой — мимо аптеки, мимо киоска с выпечкой, мимо остановки, где ветер всё время шевелил старые объявления. Иногда они заходили к Егору, ставили чайник и подолгу сидели на кухне, где за окном рано темнело, а на столе рядом с кружками лежали тетради и наскоро брошенные ручки.

Однажды разговор снова зашёл о заработке. Обычные подработки казались им слишком скучными и медленными, а хотелось чего-то более лёгкого, современного, почти не требующего усилий. Егор сказал, что в интернете главное — не столько продавать что-то, сколько создавать у людей ощущение удачной возможности. Сева сначала только усмехнулся, но потом оба открыли телефоны и начали записывать идеи. Постепенно у них сложился план: создать закрытое сообщество, куда можно вступить за небольшую сумму, а потом объяснять новым участникам, что они смогут вернуть свои деньги, если приведут ещё двоих. Тем, в свою очередь, нужно будет сделать то же самое, и процент от взносов пойдёт тем, кто присоединился раньше.

Через несколько дней у них уже была страница с аккуратной обложкой, короткими фразами про рост, развитие и новые возможности и общий чат, который постепенно начал наполняться людьми. Всё выглядело спокойно и даже солидно: сообщения, списки, таблица с именами, переводы, вопросы о том, как подключить следующих. Сева следил за перепиской и отмечал, кто за кем пришёл, а Егор больше занимался тем, как всё подать, чтобы схема казалась понятной и выгодной. В школе при этом ничего не менялось: контрольные шли одна за другой, кто-то перед уроком торопливо списывал домашнее задание, в столовой по-прежнему спорили о еде, а после звонка коридоры снова наполнялись обычным шумом.

Сначала им казалось, что всё складывается удачно. Люди вступали, задавали вопросы, переводили деньги, интересовались, когда можно приглашать новых участников. Телефон у Севы всё чаще вспыхивал от уведомлений, и это придавало происходящему какую-то взрослую серьёзность. Но со временем в чате стали появляться другие сообщения. Кто-то писал, что заплатил, но не понимает, что делать дальше. Кто-то спрашивал, откуда вообще должны появляться деньги, которые обещали в начале. А однажды один из участников добавил в переписку своего отца, и после этого всё изменилось.

На следующий день Егора с родителями вызвали в полицию, и он сразу сообщил об этом Севе по СМС. Тот прочитал сообщение дважды, потом молча положил телефон экраном вниз и посмотрел в окно, за которым начинал капать дождь.

Вопрос 4.1 (2 балла). Приведите термин, наиболее соответствующий явлению, описанному в тексте.

Ответ: Финансовая пирамида.

Пояснение. В тексте описана схема, в которой участники вносят деньги за вход, а затем должны приводить новых людей, чтобы вернуть свои вложения и получить прибыль. Доход в такой системе возникает не за счёт продажи полезного товара или реальной услуги, а в основном за счёт денег следующих участников. Именно это и является главным признаком финансовой пирамиды.

Вопрос 4.2 (3 балла). Опишите в небольшом тексте от 100 до 300 символов, что может привлечь жертв к участию в данной схеме.

Пример ответа: Жертв привлекают обещания сверхдоходов без усилий, иллюзия лёгких денег и давление знакомых. Мошенники играют на жадности и страхе упустить выгоду, маскируя схему под надёжный бизнес.

Гуманитарный блок. Задание 10.5.

Рассмотрите приведённую иллюстрацию и выполните задания к ней.

Вопрос 5.1 (2 балла). Приведите термин, используемый для описания изображённого явления.

Ответ: Дропперство.

Пояснение. На картинке показана конкретная схема прогонки денег через чужие счета/карты/телефоны. Банк России прямо описывает это так: преступники выводят деньги жертв через счета других лиц, а человек, который предоставляет для этого свою карту или счёт, становится дроппером. Именно это и видно на изображении: левая девочка получает «грязные» деньги и передаёт дальше, у второй деньги выглядят уже «чище», а затем уходят ещё дальше. Акцент на роли посредников, через которых прогоняют деньги. Это и есть логика дропперства.

Вопрос 5.2 (1 балл). Выберите статью УК РФ, которая больше всего подходит для описания явления, приведённого на изображении.

Статья 158. Кража
Статья 165. Причинение имущественного ущерба путём обмана или злоупотребления доверием
Статья 172. Незаконная банковская деятельность
Статья 172.2. Организация деятельности по привлечению денежных средств и (или) иного имущества
Статья 179. Принуждение к совершению сделки или к отказу от её совершения
Статья 186. Изготовление, хранение, перевозка или сбыт поддельных денег или ценных бумаг
Статья 187. Неправомерный оборот средств платежей
Статья 198. Уклонение физического лица от уплаты налогов, сборов и (или) физического лица — плательщика страховых взносов от уплаты страховых взносов
Статья 204. Коммерческий подкуп

Ответ: Статья 187. Неправомерный оборот средств платежей.

Пояснение. Из предложенных вариантов лучше всего подходит статья 187 УК РФ. После изменений 2025 года она прямо охватывает передачу электронного средства платежа и (или) доступа к нему другому лицу для осуществления неправомерных операций. Именно это и составляет суть дропперства: человек предоставляет свою карту, счёт, онлайн–банк или доступ к ним, чтобы через них прогоняли чужие незаконные деньги.

Вопрос 5.3 (2 балла). Приятель предложил вам принять участие в похожей схеме. Напишите в небольшом тексте от 100 до 300 символов, как бы вы ему ответили и почему.

Пример ответа: Я в таком участвовать не буду. Это дропперство, уголовное преступление. Дропперов сажают в тюрьму и блокируют счета. Никакая комиссия не стоит свободы и испорченной жизни. Лучше поискать законный способ заработать.

Кейс. При домашнем написании одной очень интересной и ответственной Олимпиады некоторые недобросовестные участники решили воспользоваться ИИ, загрузили задачи в подходящие платформы от Алисы до DeepSeekMath, получили от них решения и выдали их за свои.

Жюри Олимпиады тоже умеет пользоваться искусственным интеллектом, в частности, для распознавания работ, написанных при помощи искусственного интеллекта. Проверка идет про трём признакам. Не будем вдаваться в детали и назовём их признаки А, Б и В.

В случае, если работа содержит признак А работы ИИ, автор дисквалифицируется (работа снимается с проверки, а участник выбывает из конкурса) независимо от прочих обстоятельств. Обнаружение же признаков Б и В требует экспертизы. В случае, если экспертиза подтверждает работу ИИ, автор также дисквалифицируется.

Исследование показало, что часть участников, пользующихся ИИ, пытаются перерабатывать полученные от ИИ тексты, после чего признаки А и Б иногда исчезают или почти исчезают. При этом были получены следующие верные количественные оценки.

1) Признак А проявляется в 100% работ, выполненных ИИ, но доля недобросовестных участников, умеющих избавляться от данного признака, равна 30%.
2) Признак Б проявляется в 90% работ, сделанных с участием ИИ, и экспертиза признаёт их несомненно недобросовестными с вероятностью $0,6$.
3) Признак В проявляется в 60% работ, сделанных при помощи ИИ, и экспертиза признаёт их недобросовестными с вероятностью $0,8$.
4) Признаки А, Б и В присутствуют во всех текстах ИИ независимо друг от друга.

Проверка Олимпиады выявила, что признак А работы ИИ присутствует в 9 000 из 15 000 сданных участниками работ.

Задание 1 (5 баллов). Считая все имеющиеся оценки точными, найдите долю участников, которые писали работу честно, не прибегая к использованию ИИ.

Задание 2 (5 баллов). Считая все имеющиеся оценки точными, найдите долю дисквалифицированных среди недобросовестных участников.

Задание 3 (5 баллов). Считая все имеющиеся оценки точными, найдите долю дисквалифицированных среди тех недобросовестных участников, кто избавился от признака А работы ИИ.

Ответ: 1) $\frac{1}{7}$; **2)** прибл. $0,928$; **3)** прибл. $0,761$.

Решение. Пусть доля добросовестных участников равна p. Тогда доля недобросовестных участников равна $1-p$. Из них 30% избавились от признака А, а 70% не умеют этого делать. Их доля от общего количества равна $0,7(1-p)$. Эти работы и были выявлены во время проверки. Её результаты показывают: доля недобросовестных участников, не избавившихся от признака А, равна $9000/15000 = 0,6$. Получаем уравнение $0,7(1-p) = 0,6$, откуда $p = 1/7$.

Доля участников с какими-то параметрами совпадает с вероятностью для случайно выбранного участника иметь эти параметры. Поэтому для удобства перейдём от долей к вероятностям.

Рассмотрим участников, использовавших в своих работах ИИ. Признак А не выявляется с вероятностью $0,3$. Признак Б выявляется с вероятностью $0,9 \cdot 0,6 = 0,54$, а не выявляется — с вероятностью $1-0,54 = 0,46$. Аналогично с признаком В — вероятность его невыявления $1-0,6 \cdot 0,8 = 0,52$. Участник не дисквалифицирован, если в его работе не выявлен ни один из признаков. Их выявление происходит независимо. Поэтому вероятность невыявления ни одного из признаков равна произведению вероятностей невыявления для каждого из них: $0,3 \cdot 0,46 \cdot 0,52 = 0,07176$. Значит, вероятность дисквалификации для использовавших ИИ равна $1-0,07176 = 0,92824 \approx 0,928$.

Рассмотрим только участников, избавившихся от признака А. Для них дисквалификация происходит по признакам Б и В. Аналогично предыдущему пункту вероятность невыявления ни одного из признаков Б и В равна $0,46 \cdot 0,52 = 0,2392$. Значит, вероятность дисквалификации для избавившихся от признака А равна $1-0,2392 = 0,7608 \approx 0,761$.