III Международная олимпиада по финансовой безопасности
Задания и решения заключительного этапа
10 класс

Тематический блок 1
(математика, информатика, экономика)

Задание 1. [*5 баллов*] Поступил сигнал, что гражданин Н. в одной из комнат своей квартиры, площадью 15 м^2, хранит 250 000 ввезенных в обход таможни смартфонов в оригинальной упаковке общей стоимостью 1,2 миллиарда рублей. Следователь Иванов, не поверив данной информации, сказал, что как минимум одно из чисел ошибочно. Почему он так решил? Объясните логику его рассуждений. Считая, что ошибочным является только одно число, предложите его замену, чтобы следователь поверил сигналу. Обоснуйте свой ответ.

Задание 2. [*5 баллов*] Иван Петрович пристраивает своих друзей в подконтрольные компании, каждого – ровно в одну компанию. Он подсчитал, что если пристраивать по одному другу в каждую из фирм, то десяти друзьям не хватит мест работы, а если в каждую компанию пристраивать по два друга, то четыре компании окажутся без друзей. Сколько друзей пристраивает Иван Петрович? Обоснуйте свой ответ.

Задание 3. [*5 баллов*] Консалтинговая компания «Все включено» по каждому заключенному договору на консалтинговые услуги привлекает ровно двух субподрядчиков из своих 10 дочерних компаний, причем любые две дочерние компании одновременно привлекаются в качестве субподрядчиков не более чем по одному договору. Каждая из дочерних компаний была привлечена в рамках субподряда ровно 7 раз. Сколько договоров на консалтинговые услуги заключила компания «Все включено»? Обоснуйте свой ответ.

Задание 4. [*5 баллов*] При проведении проверки компании «Радость» были выявлены три фирмы, оказывавшие ей консалтинговые услуги: ООО «Скаляр», ООО «Вектор» и ООО «Тензор». При сверке списков сотрудников этих компаний было обнаружено, что сотрудники, работающие в ООО «Скаляр», не работают ни в ООО «Вектор», ни в ООО «Тензор» и, кроме того, ООО «Вектор» и ООО «Тензор» также не имеют общих сотрудников. Зато выяснилось, что все сотрудники компании «Радость» трудоустроены в эти три ООО по совместительству: ровно треть сотрудников «Радости» числится в ООО «Скаляр» (где сотрудники «Радости» составляют половину от всех сотрудников), ровно треть – в ООО «Вектор» (где сотрудники «Радости» составляют ровно $2/3$ от общего числа сотрудников), а ровно треть оставшихся – в ООО «Тензор» (где сотрудники «Радости» составляют ровно $3/4$ от общего числа сотрудников).

Какое наименьшее количество сотрудников могло работать в компании «Радость»? Обоснуйте свой ответ.

Задание 5. [*5 баллов*] Для оценки разброса заработных плат в организации иногда используется *децильный зарплатный коэффициент*: отношение средней заработной платы 10% самых высокооплачиваемых работников к средней заработной плате 10% самых низкооплачиваемых работников.

а) Уменьшится, увеличится или не изменится децильный зарплатный коэффициент, если увеличить всем сотрудникам зарплаты на 4%? (Можно написать только ответ.)

б) Уменьшится, увеличится или не изменится децильный зарплатный коэффициент, если увеличить всем сотрудникам зарплаты на 5 000 рублей? (Можно написать только ответ.)

в) Иногда помимо децильного зарплатного коэффициента возможно использование *квартильного зарплатного коэффициента*: отношения средней заработной платы 25% самых высокооплачиваемых работников к средней заработной плате 25% самых низкооплачиваемых работников. Докажите, что квартильный зарплатный коэффициент всегда не превосходит децильный.

Тематический блок 2
(обществознание, право)

Задание 1. Прочитайте текст и выполните задания.

(I) На сегодняшний день противодействие кибератакам является проблемой мирового масштаба. Более того, кибератаки превратились в организованный бизнес, и достаточно прибыльный, в основе которого лежит, как правило, использование вредоносного программного обеспечения. Вредоносные компьютерные программы все чаще пишутся с целью незаконного обогащения за счет их дальнейшей перепродажи, а также в целях незаконного получения конфиденциальной информации пользователей и последующего хищения принадлежащих им денежных средств.

(II) Если говорить о финансово-кредитных учреждениях, можно сказать, что здесь наиболее распространено использование современных информационных технологий и сети Интернет, причем как для удобства предоставления своим клиентам новых банковских продуктов и услуг, так и для быстроты осуществления денежных переводов, что не может не привлекать внимания злоумышленников. За 2017 г. бизнес потерял примерно 116 млрд рублей из-за кибератак – убытки из-за киберпреступников признала почти каждая пятая российская компания. Для злоумышленников кибератаки во многом привлекательны за счет того, что сегодня совершенно из любой точки земного шара они могут осуществлять подготовку и совершение кибератак, поскольку теряет в стоимости компьютерная техника, а объекты таких преступных посягательств не обязательно должны находиться в непосредственной близости от преступников. Характерно и то, что для совершения компьютерных преступлений не требуется прикладывать особые усилия и затраты, ведь достаточно иметь компьютер, программное обеспечение и подключение к информационной сети. Глубокие технические познания также не обязательны – в сети Интернет можно найти большое количество специальных форумов, закрытых чатов в мессенджерах, в которых желающий может овладеть соответствующими познаниями и навыками, приобрести вредоносное программное обеспечение для последующего совершения правонарушений, похищенные номера кредитных карт, похищенные персональные и идентификационные данные пользователей, а также объединить усилия по проведению целенаправленных компьютерных атак на компьютерные системы различных объектов.

(III) Вышеперечисленные обстоятельства крайне затрудняют расследование компьютерных преступлений, которое требует максимально оперативного анализа и сохранения данных, которые ввиду своей уязвимости могут быть легко уничтожены злоумышленниками за считанные минуты.

(IV) Актуальным остается вопрос и о территориальной юрисдикции в случае совершения правонарушения на территории другого государства. Это определяет необходимость правовой оценки действий компьютерного злоумышленника как со стороны государства, на территории которого он использовал технические устройства при совершении противоправных действий, так и государства, которому или гражданам которого причинен ущерб.

(V) Следует подчеркнуть, что чем стремительнее развивается сфера информационных технологий, тем больше новых видов правонарушений изобретают злоумышленники, которые не перестают совершенствовать свои навыки и придумывать новые способы незаконного обогащения в данной сфере. При этом государству необходимо наращивать темп проведения мероприятий, направленных на профилактику, предупреждение и борьбу с киберпреступностью, поскольку, как показывает правоприменительная практика, относительная длительность и бюрократический подход к развитию нормативно-правовой базы приводят к значительному отставанию таких мероприятий. Рост компьютерных преступлений именно в финансово-кредитной сфере требует от сотрудников правоохранительной системы не только неукоснительного соблюдения и выполнения своих непосредственных служебных обязанностей по расследованию преступлений, но также понимания банковских процессов и финансовых отношений.

(VI) Есть и другая проблема в данном направлении, связанная с программой обучения следственных и оперативных работников правоохранительной системы. Многие программы устарели и не отвечают новым вызовам.

(VII) До недавнего времени судьи, прокуроры и следователи руководствовались в своей профессиональной деятельности нормативно-правовыми документами, которые уже устарели и не дают ответов на все актуальные вопросы, что мешает представителям названных ветвей власти не только иметь правильное представление о киберпреступлениях и механизмах их совершения, но и реализовывать общий подход к толкованию и правоприменению.

(VIII) Одним из ключевых направлений обеспечения информационной безопасности является усиление государственно-частного партнерства и развитие соответствующих регионально-ориентированных программ с учетом экономической заинтересованности кредитных организаций в повышении уровня защищенности их информационных ресурсов.

(IX) Отдельно обращает на себя внимание проблема недостаточного уровня киберграмотности населения. Большинство киберпреступлений совершается, в том числе благодаря неосведомленности населения и клиентов кредитно-финансовых организаций, а также несоблюдения ими основных правил безопасности. В связи с этим значительную пользу в предупреждении киберпреступности имеют информационно-просветительские мероприятия в отношении новых рисков и угроз в информационных и компьютерных системах. Важно соблюдать элементарные правила информационной безопасности, а именно: не пренебрегать антивирусом, создавать и использовать сложные пароли, не повторять их на всех используемых ресурсах, применять двухфакторную аутентификацию везде, где это возможно, использовать функции шифрования информации на жестких дисках, USB-носителях и применять шифрование для сохранения конфиденциальности переписки в интернете.

(По материалам Савенкова Д.Д. Кибербезопасность финансово-кредитных организаций в условиях новых вызовов и угроз в цифровом пространстве // Право и государство: теория и практика. 2018. № 4.)

1.1. [*1 балл*] Укажите номер абзаца, в котором приводится термин, обозначающий пределы распространения властных полномочий государственных органов.

Ответ

1.2. [*4 балла*] Проанализируйте текст статьи и приведенные ниже публикации в СМИ. Укажите буквенные обозначения публикаций, которые соответствуют мнению автора статьи об обстоятельствах, ведущих к увеличению количества киберпреступлений и затруднению их раскрытия.

А. Мошенники размещают ссылки на зараженные архивы в обсуждениях на форумах и продвигают их в поисковых системах. Раньше вирусы на форумах распространялись под видом расширений для популярных игр или программ, но сейчас злоумышленники выдают их почти на любой запрос в сети, говорят эксперты.

Б. Подпольные криминальные форумы стали набирать популярность. В одном из сообщений на форуме хакер, ранее делившийся вредоносным ПО для Android, продемонстрировал код, написанный ChatGPT, который похищал интересующие его файлы, сжимал их и отправлял по сети. Они продемонстрировали еще один инструмент, который устанавливал на компьютер бэкдор («тайный вход» – дефект алгоритма для удаленного доступа) и мог загружать на зараженный ПК дополнительные вредоносные программы.

В. В Telegram пришел новый бот, предлагающий пользователям доступ к персональным данным россиян за небольшую плату. Об этом пишут «Известия». Сервис позволяет получать информацию о любом человеке по различным критериям, таким как Ф.И.О., телефон, ИНН, e-mail, номер автомобиля и другие. Стоимость запроса зависит от типа данных.

Г. «Утечка персональных данных является серьезной проблемой мировой, и виноват не только тот, кто украл данные, но и тот, кто, сознательно понимая, что он на черном рынке

приобретает массив персональных данных и потом их использует без права на то, должен нести ответственность», – подчеркнул глава Роскомнадзора.

Д. От возможных хакерских атак на банковские счета с перехватом СМС можно защититься с помощью усложнения настроек конфиденциальности, однако основная ответственность за безопасность денег граждан в этом случае лежит на сотовых операторах и банковских системах безопасности, заявили РБК российские эксперты в области кибербезопасности.

Е. Житель города Обь Новосибирской области при помощи компьютерного вируса украл криптовалюту у более чем 1 тыс. человек, сообщает ТАСС со ссылкой на данные пресс-службы УФСБ по региону. Мужчина покупал на закрытых интернет-сайтах вредоносные программы для кражи паролей с компьютеров пользователей, уточняется в сообщении.

Ж. Число DDoS-атак на сайты правительственных организаций с 10 по 20 мая выросло на 74% в сравнении с аналогичным периодом прошлого года, их организаторами были политически мотивированные хакеры, говорится в сообщении одной из компании по кибербезопасности.

З. Одна из ведущих больниц подверглась атаке хакеров, которые потребовали выкуп за восстановление доступа к персональным данным пациентов, заявил в понедельник мэр столицы. «Муниципальная больница подверглась серьезной кибератаке, хакеры потребовали деньги за базы данных пациентов, зашифрованных ими же. Я проинформировал Службу информации и безопасности об инциденте», – сказал он в ходе оперативного заседания управлений мэрии, которое транслировалось в социальных сетях.

Ответ.

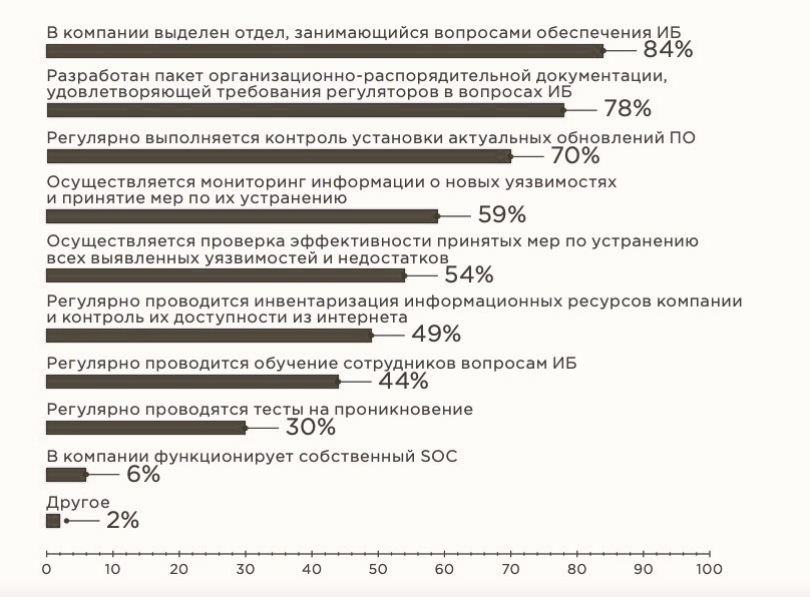
1.3. [*1 балл*] В 2021 году российская межведомственная делегация презентовала Конвенцию Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Укажите номер(-а) абзаца(-ев), в котором(-ых) автор раскрывает причину необходимости международной борьбы с киберпреступностью.

Ответ.

1.4. [*2 балла*] Ознакомьтесь с приведенной ниже инфографикой (рисунок 1 и рисунок 2). Объясните, каким образом данные, приведенные в них, соотносятся с представленной в тексте статьи информацией о киберпреступности. Приведите не менее двух объяснений.

Рисунок 1. Меры по обеспечению информационной безопасности на предприятиях.



* ИБ – информационная безопасность

** ПО – программное обеспечение

*** SOC (от англ. Security Operations Center) – центр по обеспечению информационной безопасности.

Рисунок 2. Насколько ты киберграмотен?

Ответ.

1.5. [*2 балла*] В статье автор указывает проблемы, возникающие при профилактике или расследовании киберпреступлений.

Как государство может решить проблемы, указанные в VI и VII абзацах? Предложите по одному пути решения для каждой проблемы.

Ответ.

Задание 2. Прочитайте текст и выполните задания.

Индивидуальный предприниматель Воробьев в 2020 году арендовал гаражный бокс и приступил к добыче криптовалюты. Весной 2021 года в ПАО «Россети» обратились собственники соседних гаражей с жалобой на снижение напряжения и нагрев гаражных боксов. В ходе проведенной по обращению проверки представителями ПАО «Россети» были выявлены нарушения схемы энергоснабжения по адресу гаражных боксов, выразившиеся в несанкционированном подключении энергопринимающих устройств. Сотрудники энергокомпании произвели отключение объекта от сети, вызвали сотрудников полиции. После прибытия полицейских представители ПАО «Россети» проникли в гараж, где были обнаружены устройства, предназначенные для майнинга криптовалюты. Убытки ПАО «Россети» составили более 2 млн рублей. По итогам проверки был составлен акт, который был подписан Воробьевым с отметкой «не согласен».

2.1. [*2 балла*] Выберите верные утверждения, касающиеся деятельности одного из участников приведенной выше ситуации – предпринимателя Воробьева.

А. Воробьев занимался запрещенным в России майнингом криптовалюты.

Б. Претензии ПАО «Россети» должны быть направлены к собственнику гаража, а не арендатору Воробьеву.

В. Согласно текущему законодательству Воробьев имел право заниматься майнингом криптовалюты.

Г. В связи с бездоговорным потреблением электроэнергии Воробьев неосновательно обогатился за счет ПАО «Россети».

Д. Факт получения Воробьевым энергоресурсов не является достаточным основанием для того, чтобы у него возникло обязательство по оплате этого энергоресурса.

Е. Согласно действующему законодательству, Воробьев мог заниматься только куплей-продажей криптовалюты.

Ответ.

2.2. [*1 балл*] Назовите, в рамках какого судопроизводства будет рассматриваться дело между ИП Воробьевым и ПАО «Россети».

Ответ.

2.3. [*2 балла*] Исходя из условия задания, укажите способ выявления майнеров. Назовите меру, которая может быть принята в случае выявления майнинга при отсутствии регистрации в качестве ИП.

Ответ.

2.4. [*2 балла*] Какие способы (виды) мошенничества, могут сопутствовать майнингу криптовалют? Назовите два противоправных деяния.

Ответ.

2.5. [*2 балла*] Сформулируйте два правила поведения, которые помогут избежать потерь от действия мошенников в реальной жизни, а не в виртуальном пространстве.

Ответ.

Задание 3. Ознакомьтесь со статистическими данными из аналитических справок Банка России о подозрительных операциях в банковском секторе за 2021 и 2022 годы и выполните задания.

Рисунок 1

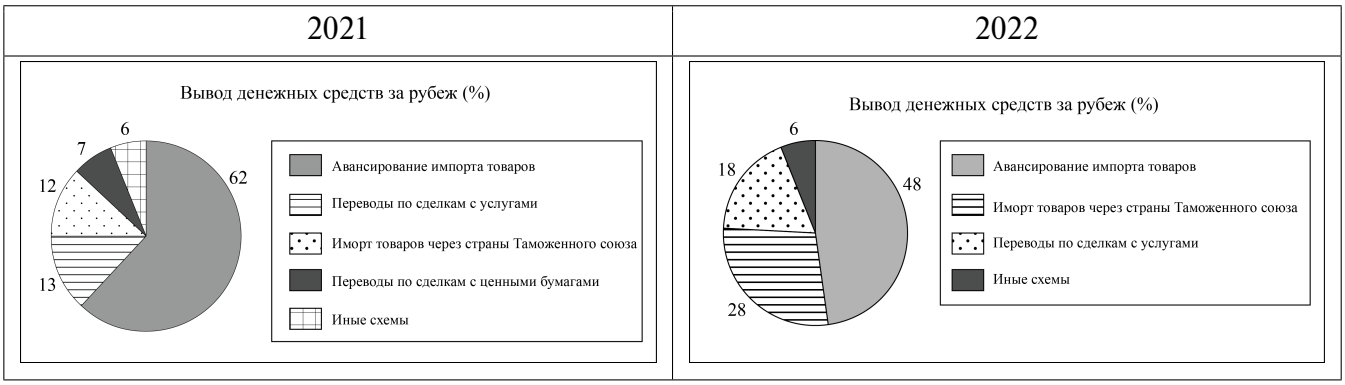


Рисунок 2

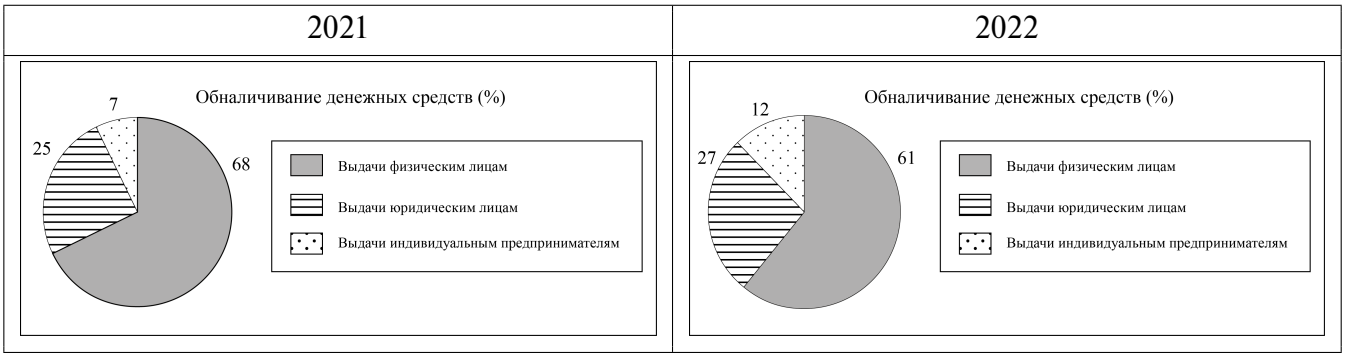
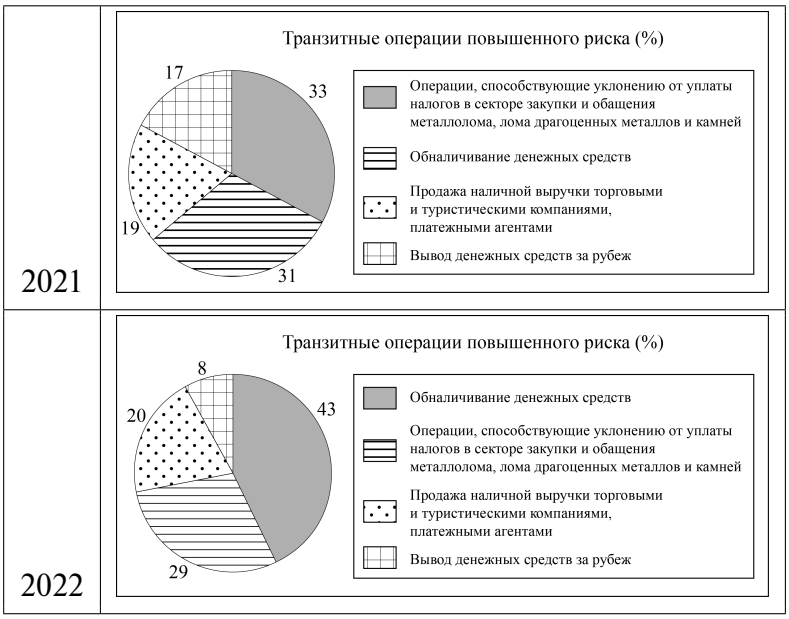


Рисунок 3



3.1. [*2 балла*] Выберите все варианты выводов, которые можно сделать на основе приведенной статистики Банка России.

А. Одним из популярных способов легализации доходов, полученных незаконным путем, в последние годы является обналичивание денежных средств.

Б. Вывод денежных средств за рубеж увеличился в два раза.

В. Доля переводов по сделкам с ценными бумагами за год уменьшилась в два раза.

Г. Доля обналичивания денежных средств юрлицами за год осталась практически неизменной.

Д. Импорт товаров через страны Таможенного союза вырос почти в три раза.

Ответ.

3.2. [*2 балла*] Отмывание денег имеет серьезные последствия как для самого общества, так и для государства. Сформулируйте два возможных последствия отмывания (легализации) доходов, полученных преступным путем.

Ответ.

3.3. [*2 балла*] В представленной выше статистике показаны возможные пути легализации доходов, полученных незаконным путем. Укажите два возможных метода борьбы с легализацией доходов, полученных преступным путем, которые могут быть использованы государством.

Ответ.

Кейс

В спальных районах крупного города расположены несколько ресторанов региональной сети «Седьмая вода». Рестораны пользуются популярностью у жителей ближайших кварталов, особенно в пятницу и субботу вечером.

Численность персонала в каждой точке невелика – от 16 до 20 штатных сотрудников кухни и зала, часть из них – студенты, которые работают официантами не каждый день.

«Седьмая вода» имеет договор эквайринга с одним из ведущих банков ОиВБ. Благодаря этому клиенты имеют возможность безналичной оплаты с помощью банковских карт всех платежных систем, действующих в России.

Сеть заключила договор с сервисом «Чайник». Через этот сервис клиент может оставить чаевые с помощью мобильного приложения или QR-кода. Это удобно клиентам, у которых нет наличных.

Ежемесячная арендная плата, покупка лицензий, оплата труда, оплата прачечной, коммунальных услуг, обслуживание и ремонт оборудования, закупка посуды и продуктов, затраты на автотранспорт – все эти операционные расходы своих ресторанов сеть «Седьмая вода» оплачивает со счета в том же банке ОиВБ. Отчетность позволяет определить, какая часть расходов приходится на каждый ресторан сети.

Выручка, прибыль и расходы сети сильно зависят от времени года. Мониторинг финансовой деятельности в летние месяцы выявил значительное падение выручки, прибыли и расходов в нескольких точках сети, в том числе в ресторане «Седьмая вода – Центр». Основные финансовые показатели работы этого ресторана за июнь–август показаны в таблице.

Статья	Июнь	Июль	Август	Примечание
Месячная выручка, р.	5 909 760	4 879 656	3 139 560	Суммы, оплаченные через карточные терминалы банка ОиВБ
Количество чеков	1440	1189	765	Чеки, выданные терминалами ОиВБ
Арендная плата, р.	960 000	900 000	900 000	Оплата со счета в банке ОиВБ
Операционные расходы (без оплаты труда и закупки продуктов), р.	967 543	765 543	356 244	Оплата со счета в банке ОиВБ
Закупка продуктов питания, р.	854 321	567 982	342 008	Оплата со счета в банке ОиВБ
Фонд оплаты труда, р.	2 446 705	2 178 215	1 656 705	Оплата со счета в банке ОиВБ
Сумма чаевых, р.	58 750	57 800	59 750	Через сервис «Чайник»
Прибыль	681 191	407 916	−175 397	

Задание 1. [*5 баллов*] Чаще всего посетители в ресторан приходят вдвоем или втроем и оплачивают весь заказ одним чеком. Известно, что в среднем на 29 посетителей приходится 10 чеков. Найдите среднюю стоимость заказа на одного посетителя за летние месяцы. Обоснуйте свой ответ.

Задание 2. [*5 баллов*] Финансового аналитика насторожило падение выручки, прибыли и операционных расходов ресторана «Седьмая вода — Центр» в течение лета, когда количество посетителей и другие условия работы ресторана не должны резко меняться. Проверка показала, что аналогичная ситуация наблюдалась еще в пяти ресторанах сети «Седьмая вода». Однако в других ресторанных сетях выручка и прибыль точек были стабильны. Является ли наблюдаемое явление основанием заподозрить мошенничество или наблюдаемые изменения можно объяснить иными причинами? Обоснуйте свой ответ.

Задание 3. [*5 баллов*] Если предположить, что наблюдаемое финансовым аналитиком явление связано с нарушением закона, то какие виды правонарушений могли быть совершены в данном случае? Назовите два правонарушения. В каком случае юридическую ответственность будут нести физические лица (сотрудники ресторана), а в каком сама организация как юридическое лицо? Если предположить, что наблюдаемое финансовым аналитиком явление связано с нарушением закона, то будут ли нести юридическую ответственность посетители ресторана? В каком правовом статусе они могут находиться в судебном процессе по делу?