



ИНТЕЛЛЕКТУАЛЬНЫЙ
МЕГАПОЛИС

ЗАДАЧНИК



Кадетский класс

В МОСКОВСКОЙ ШКОЛЕ

НАПРАВЛЕНИЕ
МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
– МИД

ПРАКТИЧЕСКИЙ ЭТАП

МОСКВА
2024



Оглавление

Вариант 1	3
Вариант 2	6
Вариант 3	9
Вариант 4	11
Вариант 5	14
Вариант 6	17
Вариант 7	19
Вариант 8	22

ВАРИАНТ 1

Задание 1.

Ознакомьтесь с фрагментом текста

20 ноября 2012 года на официальном сайте принца Уильяма, герцога Кембриджского, появились интересные фотографии, показывающие его жизнь как пилота спасательного вертолета Королевских военно-воздушных сил. Эти изображения были показаны на нескольких телеканалах и напечатаны в газетах. Однако, к сожалению, фотографы не обратили внимания на важную деталь: на одной из фотографий за спиной принца Уильяма к стене прикреплена бумажка с логином и паролем, которые можно разглядеть при зуммировании. Как выяснилось, это были учетные данные для доступа к серверу авиабазы RAF Valley, где служил принц. Более того, на некоторых фотографиях были видны экраны компьютеров с конфиденциальной информацией из внутренней компьютерной системы Королевских военно-воздушных сил.

После того как информация стала доступна, военные власти поняли, что это может стать большой проблемой. Они немедленно удалили оригиналы фотографий в высоком разрешении с сайта, а оставшиеся копии были подкорректированы в графическом редакторе, а со временем официальные источники Великобритании стали публиковать отредактированную версию этой фотографии, на которой конфиденциальная информация была скрыта. Министерство обороны Великобритании даже объявило о сбросе паролей для всех сотрудников, чтобы предотвратить возможные злоупотребления.

«Ввиду административного недосмотра эти фотографии не были корректно проверены в RAF Valley, и на них были показаны незасекреченные имена пользователей сотрудников Минобороны, а также пароли и снимки экранов системы с ограниченным доступом», - заявил представитель министерства.

Публикация этих фотографий в СМИ привела к тому, что злоумышленники получили возможность использовать этот пароль для несанкционированного доступа к внутренним системам базы. Это привело бы к компрометации конфиденциальной информации, включая данные о военнослужащих, их размещении и других критически важных аспектах работы базы. После утечки пароля военные власти начали внутреннее расследование, чтобы оценить возможные последствия и ущерб. Это привело к повышению уровня безопасности на базе, а также к пересмотру политики по управлению паролями и доступом к закрытым системам.

Вопросы к тексту:

1. Какие конкретные меры безопасности были нарушены при публикации фотографий принца Уильяма?

Ответ: При публикации фотографий принца Уильяма были нарушены несколько ключевых мер безопасности. Во-первых, на одной из фотографий был виден логин и пароль, которые использовались для доступа к серверу авиабазы RAF Valley. Это является серьезным нарушением, так как такие данные должны быть защищены и не подлежат раскрытию. Во-вторых, на некоторых фотографиях были видны экраны компьютеров с конфиденциальной информацией, что также недопустимо. Кроме того, фотографии не прошли должную проверку на наличие чувствительной информации перед публикацией, что указывает на недостаточный контроль со стороны ответственных лиц.

2. Какие меры должны быть приняты для предотвращения утечки конфиденциальной информации при публикации фотографий в социальных сетях и СМИ?

Ответ: Для предотвращения утечки конфиденциальной информации необходимо внедрить строгие процедуры проверки фотографий перед их публикацией. В первую очередь надо начать с простой

человеческой проверки фотографий на предмет чувствительной информации. Далее меры могут включать использование программного обеспечения для автоматического обнаружения чувствительных данных, таких как пароли и экраны компьютеров. Также важно обучать сотрудников, как распознавать и обрабатывать фотографии, содержащие конфиденциальную информацию. Кроме того, доступ к публикации контента должен быть ограничен только уполномоченными лицами, прошедшими обучение по кибербезопасности.

3. Какие меры должны быть предприняты для устранения последствий опубликования фотографий с чувствительной информацией?

Ответ: В целом можно отметить, что Министерство обороны все сделало правильно. После публикации фотографий с чувствительной информацией следует немедленно удалить оригиналы в высоком разрешении и опубликовать отредактированные версии, скрывающие конфиденциальные данные. Также необходимо провести внутреннее расследование для оценки возможных последствий утечки информации и ущерба. Важно сбросить все пароли, которые могли быть скомпрометированы, и выдать новые. Кроме того, следует повысить уровень безопасности систем, к которым были раскрыты пароли, и пересмотреть политики управления паролями и доступом к конфиденциальной информации.

4. Какие существуют правила надежного пароля?

Ответ: Правила надежного пароля включают создание паролей длиной не менее 12 символов, состоящих из комбинации букв верхнего и нижнего регистра, цифр и специальных символов. Необходимо избегать использования очевидных слов, дат рождения и личных данных. Также важно не использовать один и тот же пароль для разных учетных записей и регулярно менять пароли, особенно если есть подозрение на их компрометацию. Рекомендуется использовать двухфакторную аутентификацию для дополнительной защиты. Способу хранения паролей также стоит уделять отдельное внимание: он должен храниться в надежном месте или в специально защищенных приложениях.

5. Какое значение имеет обучение сотрудников по вопросам кибербезопасности, особенно для людей, работающих с секретной информацией?

Ответ: Обучение сотрудников по вопросам кибербезопасности имеет критическое значение, особенно для тех, кто работает с секретной информацией. Оно помогает повысить осведомленность о рисках и угрозах, связанных с утечкой данных. Сотрудники должны знать, как распознавать фишинговые атаки и другие методы социальной инженерии, а также понимать важность соблюдения политик безопасности. Регулярное обучение формирует культуру кибербезопасности в организации и снижает вероятность инцидентов, подобных утечке паролей принца Уильяма.

Задание 2.

Ознакомьтесь с фрагментом текста

О важности иммунитетов и привилегий в дипломатической деятельности

В результате неуплаты налогов в размере около 50 фунтов стерлингов посол Петра I при английском дворе А. А. Матвеев (1707–1708) вечером 21 июля 1708 г. был насильно задержан на улице и взят судебным приставом под стражу. Королева Анна немедленно поручила государственному секретарю выразить Андрею Артамоновичу возмущение фактом нападения на него и сообщить, что виновные будут наказаны. Не удовлетворившись этим, русский посол потребовал действительного наказания виновных. Не получив желательного удовлетворения, Матвеев уехал из Лондона в Амстердам, так и не вручив отзывных грамот.

25 июля королева выразила свое сожаление по поводу этого печального события и повелела статс-секретарю созвать чрезвычайное заседание Тайного совета для решения вопроса о наказании виновных в этом деле. После этого она лично написала Петру I и сообщила об аресте и предании суду причастных к нему купцов и судебных чиновников. Несмотря на издание особого закона об иммунитете лиц дипломатического персонала и тот факт, что парламент при амнистии по всем преступлениям, совершённым после 1695 года, специально исключил из амнистии лиц, виновных в покушении на Матвеева, Пётр I потребовал специального удовлетворения за оскорбление его посла.

Удовлетворение было представлено английской королевой в следующей форме: лорд Ч. Уитворт, чрезвычайный посланник королевы при российском дворе, был ею назначен чрезвычайным послом для принесения Петру I на торжественном собрании всего двора и дипломатического корпуса извинения королевы. 5 февраля 1709 г. Уитворт, стоя и с непокрытой головой, выразил Петру I извинения королевы.

Через четыре дня на заседании Совета министров при участии Петра I и английского посла было вынесено следующее решение: император приказывает Матвееву, своему послу в Гааге, сообщить английской королеве, что он соизволил принять извинения, принесённые от её имени, и просит помиловать виновных. Королева напишет Матвееву письмо, соответствующее обстоятельствам, и вознаградит его за понесённые расходы. Пётр I прикажет Матвееву вручить свои отзывные грамоты. Когда всё это будет исполнено, русский царь засвидетельствует английской королеве своё удовлетворение собственноручным письмом, которое будет вручено лорду Ч. Уитворту.

Вопрос: правильным ли был такой шаг со стороны Петра I и как можно охарактеризовать его.

Ответ: внешняя политика России в период царствования Петра I характеризовалась амбициозными целями и значительными достижениями – первостепенной задачей было укрепление позиций Российской империи как крупной державы и расширение ее влияния в Европе и Азии. Её важными отличительными чертами является прагматичность, жёсткость и решительность.

К этому следует добавить, что высшей целью российской дипломатии как средства внешней политики всегда являются государственный интерес и судьба человека, ее высшим профессиональным признаком – умение соединить в единое целое закон, цели, мораль и культуру.

Все это ярко прослеживается на примере изложенного выше дипломатического казуса, случившегося с Андреем Артамоновичем Матвеевым, послом Петра I при английском дворе.

ВАРИАНТ 2

Задание 1.

Ознакомьтесь с фрагментом текста

В 2011 году произошел инцидент, связанный с публикацией фотографий, на которых запечатлены высокопоставленные лица, включая президента США Барака Обаму, во время операции по ликвидации Усамы бен Ладена.

В ситуационном центре Белого дома были сделаны фотографии, на которых видно, как Обама и его советники следят за ходом операции. Однако на одной из фотографий, опубликованных в СМИ, можно было разглядеть документы и экраны компьютеров, содержащие конфиденциальную информацию о планировании операции и действиях спецподразделений.

Этот инцидент стал предметом обсуждения в СМИ, так как на фотографиях были видны детали, которые не должны были быть раскрыты широкой публике. Несмотря на то что фотографии были сделаны в рамках официального события, их публикация привлекла внимание к вопросам безопасности, поскольку на них содержались важные сведения, которые могли угрожать безопасности операций и людей, участвующих в них.

После этого инцидента администрация Обамы приняла меры для усиления безопасности и контроля за информацией, представляемой в публичном доступе.

Вопросы к тексту:

1. Какие конкретные меры безопасности были нарушены при публикации фотографий?

Ответ: При публикации фотографий были нарушены несколько ключевых мер безопасности. Во-первых, на фотографиях была конфиденциальная информация. Это является серьезным нарушением, так как такие данные должны быть защищены и не подлежать раскрытию. Во-вторых, фотографии не прошли должную проверку на наличие чувствительной информации перед публикацией, что указывает на недостаточный контроль со стороны ответственных лиц.

2. Какие меры должны быть приняты для предотвращения утечки конфиденциальной информации при публикации фотографий в социальных сетях и СМИ?

Ответ: Для предотвращения утечки конфиденциальной информации необходимо внедрить строгие процедуры проверки фотографий перед их публикацией. В первую очередь надо начать с простой человеческой проверки фотографий на предмет чувствительной информации. Далее меры могут включать использование программного обеспечения для автоматического обнаружения чувствительных данных, таких как пароли и экраны компьютеров. Также важно обучать сотрудников, как распознавать и обрабатывать фотографии, содержащие конфиденциальную информацию. Кроме того, доступ к публикации контента должен быть ограничен только уполномоченными лицами, прошедшими обучение по кибербезопасности.

3. Какие меры должны быть предприняты для устранения последствий опубликования фотографий с чувствительной информацией?

Ответ: Для устранения последствий опубликования фотографий с чувствительной информацией необходимо провести расследование инцидента, чтобы оценить ущерб и выявить уязвимости в системах безопасности. Следует уведомить все заинтересованные стороны о произошедшем и принять меры для защиты раскрытых данных. Также важно сотрудничать с правоохранительными органами и экспертами по кибербезопасности для расследования утечки и привлечения виновных к ответственности.

В дальнейшем необходимо пересмотреть политики и процедуры работы с конфиденциальной информацией, чтобы предотвратить подобные инциденты в будущем. После публикации фотографий с чувствительной информацией следует немедленно удалить оригиналы в высоком разрешении и опубликовать отредактированные версии, скрывающие конфиденциальные данные.

4. Что может произойти, если злоумышленники получают доступ к конфиденциальным данным через опубликованные фотографии, с точки зрения информационной безопасности?

Ответ: Злоумышленники могут использовать полученные данные для взлома учетных записей и систем, если на фотографиях видны пароли или логины. Это может привести к несанкционированному доступу к внутренним системам, кражам данных, финансовым потерям и другим видам мошенничества. Утечка конфиденциальной информации может нанести серьезный ущерб репутации организаций. Доступ злоумышленников к конфиденциальным данным через опубликованные фотографии представляет собой серьезную угрозу, которая может иметь далеко идущие последствия для национальной безопасности в целом.

5. Какое значение имеет обучение сотрудников по вопросам кибербезопасности, особенно для людей, работающих с секретной информацией?

Ответ: Обучение сотрудников по вопросам кибербезопасности имеет критическое значение, особенно для тех, кто работает с секретной информацией. Оно помогает повысить осведомленность о рисках и угрозах, связанных с утечкой данных. Сотрудники должны знать, как распознавать фишинговые атаки и другие методы социальной инженерии, а также понимать важность соблюдения политик безопасности. Регулярное обучение формирует культуру кибербезопасности в организации и снижает вероятность подобных инцидентов.

Задание 2.

Ознакомьтесь с фрагментом текста

О дипломатических иммунитетах и привилегиях, предоставляемых членам семей дипломатов

Французская фирма предъявила иск к жене дипломатического (коммерческого) агента Министерства финансов России во Франции Артура Германовича Рафаловича (1894-1917) в Сенском гражданском суде об уплате за поставку и ремонт автомобиля. Ответчица просила суд признать дело неподсудным ввиду того, что она является женой аккредитованного во Франции дипломатического агента. Истец указывал, что ответчица как подавшая просьбу о раздельном жительстве с мужем и получившая на это разрешение утратила свой судебный иммунитет. К мнению истца присоединился и соответчик — дипломатический агент муж Рафалович.

Тем не менее Сенский суд в своём решении от 18 сентября 1907 г. признал это дело неподсудным, исходя из следующих оснований: 1) принципиально дипломатический иммунитет распространяется на лиц из официальной свиты агента и на членов его семьи, в частности на жену; 2) совокупность мер, имеющих своим назначением обеспечение независимости и достоинства иностранных дипломатов, аккредитованных во Франции, была установлена не в их личных интересах; поэтому отказ дипломатического агента от иммунитета может быть действительным лишь в том случае, если он получит разрешение своего правительства; 3) в этом отношении не следует делать различия между официальной свитой агента и его семьёй; 4) временное раздельное жительство жены дипломатического агента не лишает её дипломатического иммунитета.

Вопрос: как Вы прокомментируете решение французского суда.

Ответ: Вопросы дипломатических иммунитетов и привилегий относятся к дипломатическому праву — одной из подотраслей права внешних сношений, которое, в свою очередь, является одной из основных отраслей международного права, представляющей собой совокупность норм, регламентирующих статус и функции государственных органов внешних сношений. Дипломатическое право регулирует правовое положение и деятельность дипломатических представительств государств и их оперативно-дипломатического состава.

Долгое время источником дипломатического права являлся международный обычай. Впервые дипломатическое право было кодифицировано в XIX веке, а именно на Венском конгрессе 1815 года и на Аахенском конгрессе 1818 года.

Согласно действовавшей на момент происшествия Декларации Аахенского конгресса 1818 года, заключённой между пятью европейскими державами и обращённой ко всем европейским дворам, указывалось, что монархи, вступившие в союз, признают своей главной, непременной обязанностью во всех отношениях, как между собой, так и с другими державами, неуклонно следовать началам международного права.

Кроме того по результатам работы конгресса был подписан протокол, дополнявший постановления Венского конгресса 1815 года о ранге дипломатических агентов и определявший место министров — резидентов ниже посланников и выше поверенных в делах.

Следующим важным актом в дипломатическом праве стала Гаванская конвенция о дипломатических чиновниках 20 февраля 1928 года. Ныне основным договорным актом в области дипломатического права является Венская конвенция о дипломатических сношениях 1961 года. В 1969 году на Генеральной ассамблее ООН была также принята Конвенция о специальных миссиях, а в 1975 году на дипломатической конференции в Вене — Конвенция о представительстве государств в их отношениях с международными организациями универсального характера.

ВАРИАНТ 3

Задание 1.

Ознакомьтесь с фрагментом текста

В 2020 году российская игровая компания "Mail.ru Group" столкнулась с серьезной кибератакой на свою популярную многопользовательскую онлайн-игру "Warface". Игра, которая имеет международную аудиторию, позволяет игрокам из разных стран участвовать в командных сражениях и выполнять различные миссии.

В ходе атаки злоумышленники использовали уязвимости в системе безопасности игры для получения доступа к личным данным игроков, включая имена, адреса электронной почты и информацию о платежах. В результате утечки данных пользователи начали получать фишинговые письма, которые выглядели как официальные уведомления от "Warface", с просьбой подтвердить свои учетные данные.

Компания "Mail.ru Group" немедленно отреагировала на инцидент, уведомив пользователей о произошедшей утечке и предложив им изменить пароли и активировать двухфакторную аутентификацию. Также была проведена проверка безопасности всех систем и обновление программного обеспечения для устранения выявленных уязвимостей.

Чтобы предотвратить подобные инциденты в будущем, "Mail.ru Group" начала сотрудничество с международными экспертами по кибербезопасности и внедрила новые протоколы безопасности, включая регулярные аудиты и обучение сотрудников по вопросам защиты данных. Благодаря этим мерам компании удалось восстановить доверие пользователей, и игра продолжила развиваться на международном рынке.

Вопросы к тексту:

1. Какова была основная причина кибератаки на "Warface"?

Ответ: Основной причиной кибератаки на "Warface" стали уязвимости в системе безопасности игры, которые злоумышленники использовали для получения доступа к личным данным пользователей. Недостаточная защита данных в процессе разработки и запуска игры привела к утечке информации.

2. Какие меры предприняла компания "Mail.ru Group" для устранения последствий инцидента?

Ответ: Компания "Mail.ru Group" уведомила пользователей о произошедшей утечке данных и предложила им изменить пароли и активировать двухфакторную аутентификацию. Также была проведена проверка безопасности всех систем, обновлено программное обеспечение для устранения уязвимостей и начато сотрудничество с международными экспертами по кибербезопасности.

3. Какое значение имеет обучение пользователей по вопросам кибербезопасности для игровой компании?

Ответ: Обучение пользователей по вопросам кибербезопасности имеет критическое значение для игровой компании, так как информированные пользователи могут лучше защищать свои аккаунты и данные. Знания о том, как распознавать фишинговые атаки и следовать протоколам безопасности, помогают снизить риски утечек данных и обеспечивают безопасность операций компании. Это также способствует формированию культуры безопасности среди игроков.

4. Какие меры по обеспечению кибербезопасности должны быть приняты компанией "Mail.ru Group" для защиты своих игр?

Ответ: Компания "Mail.ru Group" должна внедрять комплексные меры по обеспечению кибербезопасности, включая: регулярное тестирование на уязвимости и устранение выявленных проблем в системах безопасности игр, использование шифрования и других криптографических методов для защиты данных игроков, внедрение многофакторной аутентификации для доступа к аккаунтам игроков, резервное копирование данных и планы восстановления после кибератак, обучение сотрудников по вопросам кибербезопасности и тестирование их готовности, сотрудничество с международными экспертами и государственными организациями для обмена информацией об угрозах.

5. Какие российские законы могли быть нарушены в результате утечки данных игроков "Warface"?

Ответ: В результате утечки данных игроков "Warface" могли быть нарушены следующие российские законы: Федеральный закон "О персональных данных" (№ 152-ФЗ), Федеральный закон "О информации, информационных технологиях и о защите информации" (№ 149-ФЗ), Федеральный закон "Об электронной подписи" (№ 63-ФЗ): Если в процессе утечки данных использовалась электронная подпись для подтверждения транзакций или идентификации пользователей, это также может быть нарушением данного закона, который регулирует использование и защиту электронных подписей, Федеральный закон "О защите прав потребителей" (№ 2300-1), если утечка данных привела к негативным последствиям для пользователей, Уголовный кодекс Российской Федерации в зависимости от характера утечки и последствий для пользователей, действия злоумышленников могут подпадать под статьи, касающиеся киберпреступлений, таких как несанкционированный доступ к компьютерной информации (статья 272 УК РФ) и распространение вредоносных программ (статья 273 УК РФ) и др.

Задание 2.

Ознакомьтесь с фрагментом текста

Когда дипломатические иммунитеты не действуют

В 1867 году в здании посольства Русской империи в Париже русский подданный Никитченков совершил покушение на убийство работника посольства Б. Французский суд приговорил Никитченкова к пожизненному тюремному заключению. Ввиду того, что преступление было совершено русским подданным в помещении посольства России, русское правительство потребовало его выдачи для суда в России.

Французский суд отклонил это требование со следующей мотивировкой: «Фикция международного права, согласно которой дом посла считается продолжением территории его суверена, защищает только дипломатических агентов и их слуг. Это не исключает юрисдикции французских судов в случае преступлений, совершённых в таком помещении лицом, не принадлежащим к посольству, хотя бы это лицо было подданным того государства, которым данный посол аккредитован».

Вопрос: Ваш комментарий относительно решения французского суда.

Ответ: Согласно действовавшим на момент происшествия положениям Протокола Аахенского конгресса 1818 года и Постановления Венского конгресса 1815 года дипломатические иммунитеты и привилегии касались только дипломатических представительств, лиц их возглавляющих и сотрудников оперативно-дипломатического состава.

Эти положения остались без изменений в последующих международных документах дипломатического права: Гаванской конвенции о дипломатических чиновниках 1928 года, Венской конвенции о дипломатических сношениях 1961 года, Конвенции о специальных миссиях 1969 года и Конвенции о представительстве государств в их отношениях с международными организациями универсального характера 1975 года.

ВАРИАНТ 4

Задание 1.

Ознакомьтесь с фрагментом текста

В 2013 году произошел значительный киберинцидент, связанный с популярной многопользовательской онлайн-игрой "League of Legends", разработанной компанией Riot Games. Инцидент начался с того, что злоумышленники рассылали фишинговые письма, которые выглядели как официальные уведомления от Riot Games. В этих письмах содержались ссылки на поддельные сайты, где игроков просили ввести свои учетные данные, такие как логины и пароли. Многие пользователи, не подозревая об обмане, раскрыли свои данные, что позволило хакерам получить доступ к их аккаунтам в игре. Таким образом, злоумышленники смогли обманным путем заполучить учетные данные игроков "League of Legends" и получить несанкционированный доступ к их аккаунтам и личной информации.

В результате фишинговой атаки были скомпрометированы данные около 339,000 игроков, включая адреса электронной почты, зашифрованные пароли, имена пользователей и даты рождения. Утечка данных стала серьезным ударом по репутации Riot Games и вызвала беспокойство среди игроков.

После инцидента Riot Games оперативно отреагировала на ситуацию и усилила меры безопасности.

Вопросы к тексту:

1. Какова была основная причина кибератаки на "League of Legends"?

Ответ: Основной причиной кибератаки стали фишинговые письма, которые злоумышленники рассылали игрокам, выдавая себя за официальные уведомления от Riot Games. Также причинами кибератаки на "League of Legends" стали уязвимости в системе безопасности игры, которые злоумышленники использовали для получения доступа к личным данным пользователей. Недостаточная защита данных в процессе разработки и запуска игры привела к утечке информации.

2. Какие меры должны была предпринять компания "Riot Games" для устранения последствий инцидента?

Ответ: Компания должна была провести внутреннее расследование, уведомить пользователей о произошедшей утечке данных и предложить им изменить пароли и активировать двухфакторную аутентификацию, провести проверку безопасности всех систем, обновить программное обеспечение для устранения уязвимостей и начать сотрудничество с правоохранительными органами и экспертами по кибербезопасности. Также Riot Games могла бы рассмотреть возможность проведения кампаний по повышению осведомленности пользователей о фишинговых атаках и других киберугрозах.

3. Какое значение имеет обучение пользователей по вопросам кибербезопасности для игровой компании?

Ответ: Обучение пользователей по вопросам кибербезопасности имеет критическое значение для игровой компании, так как информированные пользователи могут лучше защищать свои аккаунты и данные. Знания о том, как распознавать фишинговые атаки и следовать протоколам безопасности, помогают снизить риски утечек данных и обеспечивают безопасность операций компании. Это также способствует формированию культуры безопасности среди игроков.

4. Какие меры по обеспечению кибербезопасности должны быть приняты компанией "Riot Games" для защиты своих игр?

Ответ: Компания "Riot Games" должна внедрять комплексные меры по обеспечению кибербезопасности, включая: регулярное тестирование на уязвимости и устранение выявленных проблем в системах безопасности игр, использование шифрования и других криптографических методов для защиты данных игроков, внедрение многофакторной аутентификации для доступа к аккаунтам игроков, резервное копирование данных и планы восстановления после кибератак, обучение сотрудников по вопросам кибербезопасности и тестирование их готовности, сотрудничество с международными экспертами и государственными организациями для обмена информацией об угрозах.

5. Какие российские законы могли быть нарушены в результате утечки игроков "Riot Games" – граждан России?

Ответ: В результате утечки данных игроков "Riot Games" могли быть нарушены следующие российские законы: Федеральный закон "О персональных данных" (№ 152-ФЗ), Федеральный закон "О информации, информационных технологиях и о защите информации" (№ 149-ФЗ), Федеральный закон "Об электронной подписи" (№ 63-ФЗ): Если в процессе утечки данных использовалась электронная подпись для подтверждения транзакций или идентификации пользователей, это также может быть нарушением данного закона, который регулирует использование и защиту электронных подписей, Федеральный закон "О защите прав потребителей" (№ 2300-1), если утечка данных привела к негативным последствиям для пользователей, Уголовный кодекс Российской Федерации в зависимости от характера утечки и последствий для пользователей, действия злоумышленников могут подпадать под статьи, касающиеся киберпреступлений, таких как несанкционированный доступ к компьютерной информации (статья 272 УК РФ) и распространение вредоносных программ (статья 273 УК РФ) и др.

Задание 2.

Ознакомьтесь с фрагментом текста

Дипломатические иммунитеты и деятельность, несовместимая со статусом дипломата

Вышедшая 25 января 1957 года газета «Известия» сообщила о том, что накануне житель г. Ленинграда Хмелевский М. И., проходивший по Политехнической улице, обратил внимание на подозрительное поведение двух мужчин, которые остановились напротив одного из оборонных объектов города. Хмелевский заметил, что один из них распахнул свое пальто и направил в сторону объекта фотоаппарат. Второй гражданин стал прикрывать его, делая вид, что дает ему прикурить.

На эти подозрительные действия Хмелевский обратил внимание проходившего мимо Кавалкина М. Т., который подошел к неизвестным людям и, поинтересовавшись, чем они занимаются, указал на то, что фотографировать данный объект нельзя. Фотографировавший объект гражданин попытался закрыть отвороты пальто, но Кавалкин дотронулся до того места, где был фотоаппарат. Неизвестный оттолкнул его, и тот упал на проезжую часть. В этот момент у этого неизвестного лица из-под полы выпал фотоаппарат, который был подобран жителями Ленинграда и передан подошедшему в это время к ним сотруднику милиции капитану Митрофанову. Последний попросил неизвестных и свидетелей пройти в 19-е отделение милиции, где было установлено, что неизвестными являются сотрудники аппарата военно-морского атташе при посольстве США в Москве капитан П. Р. Уффелман и лейтенант У. С. Луис. Поскольку свидетели показали, что Уффелман и Луис занимались фотографированием объекта, имеющего оборонное значение, пленка была изъята из фотоаппарата. После этого П. Р. Уффелман и У. С. Луис покинули 19-е отделение милиции. Проявление позже пленки подтвердило, что они действительно фотографировали режимный объект, то есть занимались разведывательной деятельностью.

7 февраля 1957 года Министерство иностранных дел СССР в ноте посольству США в Москве сообщило, что сотрудники посольства Уффелман и Луис были застигнуты советскими гражданами во

время фотографирования режимного объекта, то есть занимались разведывательной деятельностью. По заявлению МИД СССР их дальнейшее пребывание в СССР стало нежелательным, и они были выдворены из СССР.

Вопрос: что лежало в основе принятого МИД СССР решения о выдворении двух американских военных дипломатов из страны?

Ответ: Венская конвенция о дипломатических сношениях 1961 года, как и более ранние акты, устанавливает, что все лица, пользующиеся иммунитетом, обязаны уважать законы и постановления государства пребывания, они обязаны не вмешиваться во внутренние дела этого государства (ст. 41).

Дипломатические агенты не должны заниматься в государстве пребывания профессиональной или коммерческой деятельностью в целях личной выгоды (ст. 42).

Однако многие западные государства грубо и цинично попирают нормы международного права, очень часто используют дипломатический иммунитет своих посольств и миссий и своих дипломатических представителей в других государствах для шпионажа, диверсий и другой подрывной деятельности, а также для совершения других преступлений (контрабанды, спекуляции и т. д.).

Об этом свидетельствует случай, произошедший с помощниками военно-морского атташе США капитаном Уффелманом и лейтенантом Луисом, которые занимались деятельностью, несовместимой со статусом аккредитованных дипломатических работников.

ВАРИАНТ 5

Задание 1.

Ознакомьтесь с фрагментом текста

Взлом Sony Pictures, произошедший 24 ноября 2014 года, стал одним из самых громких инцидентов в истории кибербезопасности. Этот случай привлек внимание не только из-за масштабов утечки данных, но и из-за политического контекста, связанного с выходом фильма «Интервью», который высмеивал северокорейского лидера Ким Чен Ына. Причины взлома были напрямую связаны с выходом комедии «Интервью», в которой обсуждался план покушения на Ким Чен Ына.

Хакеры, которые назвали себя «Guardians of Peace» (GOP), потребовали от Sony отменить прокат фильма, угрожая раскрыть конфиденциальную информацию о компании. В ходе атаки хакеры использовали вредоносное ПО, которое привело к уничтожению данных на серверах Sony и массовому удалению файлов. Это было описано как «компьютерное убийство», поскольку атака не только привела к утечке данных, но и фактически парализовала работу компании. Основным способом взлома были фишинговые письма, которые были отправлены сотрудникам Sony. В результате атаки хакеры смогли похитить личные данные сотрудников, включая имена, даты рождения, номера социального страхования, а также информацию о заработной плате и копии неизданных фильмов.

Эти данные были опубликованы в интернете, что нанесло серьезный ущерб репутации Sony Pictures. Последствия взлома были катастрофическими. Компания понесла значительные финансовые убытки, оцениваемые в десятки миллионов долларов, и была вынуждена инвестировать в восстановление своих систем безопасности.

Кроме того, инцидент привел к ухудшению отношений между США и Северной Кореей, так как спецслужбы США обвинили правительство КНДР в организации атаки. Несмотря на это, северокорейские власти официально отвергли обвинения, но заявили, что атака была «справедливым наказанием» для Sony.

Вопросы к тексту:

1. Каковы были основные причины кибератаки на Sony Pictures?

Ответ: Основными причинами кибератаки на Sony Pictures стали: 1) выход комедийного фильма "Интервью", в котором обсуждался план покушения на северокорейского лидера Ким Чен Ына. Это вызвало недовольство северокорейских властей, которые пригрозили последствиями; 2) использование вредоносного ПО и фишинговых писем, которые были отправлены нескольким сотрудникам. Эти письма содержали вредоносные ссылки, что позволило злоумышленникам получить доступ к внутренним системам компании.

2. Какие последствия понесла компания в результате кибератаки?

Ответ: Компания Sony Pictures понесла следующие последствия: 1) были похищены личные данные сотрудников, включая имена, даты рождения, номера социального страхования, информацию о заработной плате. 2) были украдены копии неизданных фильмов, которые затем были опубликованы в интернете, нанеся серьезный ущерб репутации компании. 3) Sony понесла значительные финансовые убытки, оцениваемые в десятки миллионов долларов, и была вынуждена инвестировать в восстановление своих систем безопасности.

3. Какие меры должны предпринять компания для устранения последствий подобной кибератаки?

Ответ: Для устранения последствий кибератаки Sony Pictures должна была: 1) провести расследование инцидента, чтобы оценить ущерб и выявить уязвимости в системах безопасности, 2) восстановить данные и системы, поврежденные в результате атаки, 3) уведомить пострадавших сотрудников и клиентов о произошедшем инциденте и предпринять меры для защиты их данных, 4) сотрудничать с правоохранительными органами и экспертами по кибербезопасности для расследования атаки и привлечения виновных к ответственности.

4. Какие меры по обеспечению кибербезопасности должны быть приняты для защиты своих информационных систем?

Ответ: Для защиты информационных систем от подобных атак компаниям необходимо внедрять комплексные меры по обеспечению кибербезопасности, включая: внедрение строгих политик управления доступом и использования паролей, регулярное обновление программного обеспечения и систем безопасности, использование многофакторной аутентификации для доступа к критически важным системам, шифрование данных в состоянии покоя и при передаче, резервное копирование данных и планы восстановления после аварий, обучение сотрудников по вопросам кибербезопасности и тестирование их готовности, сотрудничество с отраслевыми ассоциациями и правоохранительными органами для обмена информацией об угрозах.

5. Что такое фишинг и как он был использован во взломе Sony Pictures?

Ответ: Фишинг - это метод социальной инженерии, при котором злоумышленники пытаются обманом получить конфиденциальную информацию, такую как пароли или данные кредитных карт. В случае с Sony Pictures хакеры использовали фишинговые письма, которые были отправлены сотрудникам компании. Эти письма выглядели как обычные сообщения, но содержали вредоносные файлы. Когда сотрудники открывали вложения, вирус активировался и позволял хакерам получить доступ к внутренним системам Sony.

Задание 2.

Ознакомьтесь с фрагментом текста

О строгих правилах приветствия

Во время визита в марте 2016 года Барака Обамы на Кубу, который преподносился американскими средствами массовой информации как историческое событие, 44-й президент США в какой-то момент решил, что на Острове свободы он не просто почётный гость, но и человек, который своим визитом сделал большой подарок всем кубинцам. После совместной пресс-конференции с Раулем Кастро он попытался «по-дружески» похлопать кубинского лидера по плечу. Но не вышло — Рауль Кастро, заприметив этот жест, довольно ловко перехватил руку Обамы в воздухе и ... сам помахал ей.

Позже изображение, на котором кубинский лидер Рауль Кастро схватил его за запястье и поднял вверх неловко вывернутую руку президента США, стало самой тиражируемой фотографией визита в американских СМИ и соцсетях.



Местные комментаторы в шутку предположили, что Кастро, возможно, таким образом отомстил Обаме за пресс-конференцию, в ходе которой последний затронул неудобные вопросы о политических заключенных и правах человека на Острове Свободы.

Вопрос: что думаете Вы относительно действий лидеров Кубы и США?

Ответ: В государственном, дипломатическом и деловом протоколе и этикете существует строгое правило, в соответствии с которым мужчины приветствуют друг друга или обмениваются любезностями через рукопожатие. С женщинами же не принято здороваться за руку, но, если она протягивает руку мужчине первой, следует пожать её, но не так крепко, как мужчинам.

Рауль Кастро поступил совершенно правильно. Любое дипломатическое общение, тем более на высшем уровне, не допускает фамильярности и панибратства: равный разговаривает с равным. Судя по всему, своим жестом Обама хотел показать, что он статусом выше.

ВАРИАНТ 6

Задание 1.

Ознакомьтесь с фрагментом текста

В 2020 году компания Microsoft столкнулась с серьезными кибератаками, которые произошли в результате фишинговых писем, направленных на сотрудников. Эти атаки стали особенно актуальными в условиях пандемии COVID-19, когда многие сотрудники стали работать удаленно.

Хакеры отправляли сообщения, которые выглядели как официальные уведомления от IT-отдела компании, с просьбой обновить учетные данные или подтвердить информацию о безопасности. Эти письма содержали ссылки на поддельные страницы входа в систему Microsoft, которые имитировали настоящие страницы, что делало их особенно убедительными. Когда сотрудники вводили свои логины и пароли на этих фальшивых страницах, злоумышленники получали доступ к их учетным записям и могли использовать их для дальнейших атак. Это привело к компрометации личной информации и данных о клиентах, а также к утечкам конфиденциальной информации. В результате атаки хакеры могли использовать украденные учетные данные для дальнейших атак на системы клиентов, что увеличивало вероятность компрометации их данных. Кроме того, инцидент подорвал доверие клиентов к Microsoft как к поставщику услуг.

В результате этой атаки Microsoft понесла серьезные потери и усилила свои меры безопасности.

Вопросы к тексту:

1. Каковы были основные причины кибератаки на Microsoft?

Ответ: Основной причиной кибератаки стали фишинговые письма, которые злоумышленники рассылали сотрудникам Microsoft, а также уязвимости в системе безопасности компании.

2. Какие последствия понесла компания в результате кибератаки?

Ответ: В результате кибератаки Microsoft понесла серьезные последствия. Во-первых, атака привела к компрометации личной информации сотрудников и клиентов, что создало риск утечек конфиденциальных данных. Во-вторых, инцидент подорвал доверие клиентов к Microsoft как к поставщику услуг, так как пользователи стали более обеспокоенными безопасностью своих данных. В-третьих, компания понесла финансовые потери, связанные с необходимостью инвестировать в восстановление систем безопасности и улучшение защиты данных.

3. Какие меры должны предпринять компания для устранения последствий подобной кибератаки?

Ответ: Для устранения последствий кибератаки компания должна была: 1) провести расследование инцидента, чтобы оценить ущерб и выявить уязвимости в системах безопасности, 2) восстановить данные и системы, поврежденные в результате атаки, 3) уведомить пострадавших сотрудников и клиентов о произошедшем инциденте и предпринять меры для защиты их данных, 4) сотрудничать с правоохранительными органами и экспертами по кибербезопасности для расследования атаки и привлечения виновных к ответственности.

4. Какие меры по обеспечению кибербезопасности должны быть приняты для защиты своих информационных систем?

Ответ: Для защиты информационных систем от подобных атак компаниям необходимо внедрять комплексные меры по обеспечению кибербезопасности, включая: внедрение строгих политик управления доступом и использования паролей, регулярное обновление программного обеспечения и систем

безопасности, использование многофакторной аутентификации для доступа к критически важным системам, шифрование данных в состоянии покоя и при передаче, резервное копирование данных и планы восстановления после аварий, обучение сотрудников по вопросам кибербезопасности и тестирование их готовности, сотрудничество с отраслевыми ассоциациями и правоохранительными органами для обмена информацией об угрозах.

5. Что такое фишинг и как он был использован во взломе Microsoft?

Ответ: Фишинг - это метод социальной инженерии, при котором злоумышленники пытаются обманом получить конфиденциальную информацию, такую как пароли или данные кредитных карт. В случае с Microsoft хакеры использовали фишинговые письма, которые были отправлены сотрудникам компании. Эти письма выглядели как обычные сообщения, но содержали вредоносные файлы. Когда сотрудники открывали вложения, вирус активировался и позволял хакерам получить доступ к внутренним системам Microsoft.

Задание 2.

Ознакомьтесь с фрагментом текста

Супруги лидеров государств не освобождаются от выполнения норм и правил дипломатического протокола и этикета

21–22 октября 2019 года президент Украины Владимир Зеленский находился в Японии, куда был приглашен для участия в интронизации Нарухито, который стал сто двадцать шестым японским императором вместо своего отца, бывшего императора Акихито, который отрекся от престола 30 апреля того же года.

На приём у императора Японии Нарухито по этому случаю он был приглашен вместе с супругой, которая была одета в платье и перчатки лимонного цвета, из-за чего её обвинили в неуважении к монарху. Большинство наблюдателей посчитали, что так делать было нельзя, поскольку жёлтый цвет — прерогатива лишь членов самого императорского дома Страны восходящего солнца, а всем остальным носить одежду такого окраса просто непозволительно.

Но некоторые эксперты посчитали, что ничего катастрофического в ситуации с платьем и перчатками первой леди Незалежной нет в принципе, поскольку зародившееся в XIII веке правило о «цветовом разделении» в Японии сегодня юридически не действует.

Вопрос: а что думаете Вы по этому поводу? Можно ли обвинять жену Зеленского в неуважении к императору Японии?

Ответ: согласно историческим фактам, запрещенные цвета появились в Японии в VIII веке. Их использование традиционно формально под запретом и сейчас, однако это не закреплено в законе. Так, одежду лимонного цвета мог носить лишь император, и традиция красить его церемониальный наряд в этот цвет сохранилась до сих пор.

Безусловно, данное нарушение вряд ли можно считать серьезным, в современной истории немало примеров, когда нарушения дипломатического этикета были куда более существенными. Но тем не менее национальные особенности нужно всегда учитывать, поскольку каждый народ имеет свои обычаи, традиции, свою культуру и манеру общения. И японцы здесь не исключение, они особенно привержены традициям.

ВАРИАНТ 7

Задание 1.

Ознакомьтесь с фрагментом текста

В 2012 году крупнейшая нефтяная компания в мире Saudi Aramco подверглась одной из самых масштабных кибератак в истории. Атака была проведена группой хакеров, известной как "Меч Справедливости", которые взяли на себя ответственность за нападение.

Атака началась с того, что один из сотрудников с привилегированным доступом открыл фишинговое письмо, содержащее вредоносное ПО. Слабые меры защиты компьютерных систем также сыграли свою роль: вирус Shamoon, использованный в атаке, быстро распространился по сети компании, заражая машины и перезаписывая их главную загрузочную запись, что делало машины непригодными для использования.

В результате атаки вирус уничтожил данные более чем на 30,000 рабочих станций и серверов, что привело к значительным сбоям в работе компании. Атака также привела к краже конфиденциальных данных, включая электронные письма и документы, которые позже были опубликованы в Интернете.

Инцидент продемонстрировал уязвимость критически важной инфраструктуры и необходимость улучшения мер кибербезопасности, он нанес значительный ущерб компании и Saudi Aramco была вынуждена предпринять ряд мер для повышения безопасности.

Вопросы к тексту:

1. Каковы были основные причины кибератаки?

Ответ: Основной причиной кибератаки стали фишинговые письма, которые злоумышленники рассылали сотрудникам, а также уязвимости в системе безопасности компании.

2. Какие последствия понесла компания в результате кибератаки?

Ответ: В результате кибератаки компания понесла серьезные последствия. Во-первых, атака привела к компрометации личной информации сотрудников и клиентов, что создало риск утечек конфиденциальных данных. Во-вторых, инцидент подорвал доверие клиентов к компании как к поставщику услуг, так как пользователи стали более обеспокоенными безопасностью своих данных. В-третьих, компания понесла финансовые потери.

3. Какие меры должны предпринять компания для устранения последствий подобной кибератаки?

Ответ: Для устранения последствий кибератаки компания должна была: 1) провести расследование инцидента, чтобы оценить ущерб и выявить уязвимости в системах безопасности, 2) восстановить данные и системы, поврежденные в результате атаки, 3) уведомить пострадавших сотрудников и клиентов о произошедшем инциденте и предпринять меры для защиты их данных, 4) сотрудничать с правоохранительными органами и экспертами по кибербезопасности для расследования атаки и привлечения виновных к ответственности.

4. Какие меры по обеспечению кибербезопасности должны быть приняты для защиты своих информационных систем?

Ответ: Для защиты информационных систем от подобных атак компаниям необходимо внедрять комплексные меры по обеспечению кибербезопасности, включая: внедрение строгих политик управления доступом и использования паролей, регулярное обновление программного обеспечения и систем безопасности, использование многофакторной аутентификации для доступа к критически важным

системам, шифрование данных в состоянии покоя и при передаче, резервное копирование данных и планы восстановления после аварий, обучение сотрудников по вопросам кибербезопасности и тестирование их готовности, сотрудничество с отраслевыми ассоциациями и правоохранительными органами для обмена информацией об угрозах.

5. Что такое фишинг и как он был использован во взломе Saudi Aramco?

Ответ: Фишинг - это метод социальной инженерии, при котором злоумышленники пытаются обманом получить конфиденциальную информацию, такую как пароли или данные кредитных карт. В случае с Microsoft хакеры использовали фишинговые письма, которые были отправлены сотрудникам компании. Эти письма выглядели как обычные сообщения, но содержали вредоносные файлы. Когда сотрудники открывали вложения, вирус активировался и позволял хакерам получить доступ к внутренним системам Microsoft.

Задание 2.

Ознакомьтесь с фрагментом текста

Дипломатический протокол и этикет и правила вежливости

На саммите АТЭС, состоявшемся в Китае в 2014 году, президент РФ Владимир Путин, заметив, что супруга председателя КНР Си Цзиньпина Пэн Лиюань ёжится от холода, решил проявить заботу и укрыл её пледом. Первая леди Китая Пэн Лиюань дипломатично вышла из затруднительной ситуации: она поблагодарила Путина, незаметно уронив плед на руки своему помощнику, а затем позволила тому помочь надеть на себя свое пальто.



Фото: Getty Images

По мнению Foreign Policy, своим неоднозначным жестом Путин нарушил нормы и правила дипломатии. Британская Daily Mail, в свою очередь, писала, что своим знаком внимания российский лидер, напротив, решил обаять своих китайских друзей.

Ли Син, директор направления «Россия и Центральная Азия» Шанхайского института международных исследований, считает, что Путин не совершил ничего, что выходило бы за рамки дипломатического этикета, показав себя «настоящим русским». «Для джентльмена в России, где холода не редкость, нет ничего необычного в проявлении заботы о дамах в общественных местах, они могут

помогать им надевать или снимать верхнюю одежду, и это в порядке вещей, – подчеркнул Ли Син. – Другое дело, что в Китае к такому не привыкли».

Вопрос: А что думаете Вы по этому поводу?

Ответ: с точки зрения дипломатического протокола и этикета жест российского президента не является нарушением его норм и правил. Известно, что не бывает правил без исключений, и в данном случае это исключение можно рассматривать как нормальный джентльменский поступок, направленный на проявление заботы. Хорошие, вежливые манеры всегда приветствуются в дипломатии.

ВАРИАНТ 8

Задание 1.

Ознакомьтесь с фрагментом текста

Кибератака на Colonial Pipeline, произошедшая в мае 2021 года, стала одним из самых значительных инцидентов в области кибербезопасности в США. Атака была осуществлена хакерской группой под названием DarkSide, которая использовала вредоносное программное обеспечение для шифрования данных и требовала выкуп за восстановление доступа к системам.

Атака началась 7 мая 2021 года, когда хакеры получили доступ к сети Colonial Pipeline через скомпрометированный пароль для VPN. Этот доступ был возможен благодаря отсутствию многофакторной аутентификации, что облегчило злоумышленникам проникновение в систему. После получения доступа, хакеры украли около 100 гигабайт данных и внедрили ransomware, что привело к отключению трубопровода на пять дней.

Colonial Pipeline, являющаяся крупнейшей трубопроводной системой в США, отвечает за транспортировку почти половины топлива, потребляемого на Восточном побережье, включая бензин, дизельное топливо и авиакеросин. В результате атаки произошли серьезные сбои в поставках топлива, что вызвало панику среди потребителей, и многие автозаправочные станции на Восточном побережье столкнулись с дефицитом топлива. Средние цены на бензин резко возросли, а президент США Джо Байден объявил чрезвычайное положение, чтобы облегчить транспортировку нефтепродуктов и предотвратить дальнейшие перебои.

Colonial Pipeline приняла решение заплатить хакерам выкуп в размере 75 биткойнов, что на тот момент составляло около 4,4 миллиона долларов, чтобы ускорить восстановление доступа к своим системам.

После инцидента государственные органы начали принимать меры для укрепления безопасности трубопроводных сетей и других объектов критической инфраструктуры.

Вопросы к тексту:

1. Каковы были основные причины кибератаки?

Ответ: Основными причинами кибератаки на Colonial Pipeline стали недостаточные меры безопасности, в частности отсутствие многофакторной аутентификации для доступа через VPN.

2. Какие последствия понесла Colonial Pipeline в результате кибератаки?

Ответ: В результате кибератаки Colonial Pipeline понесла серьезные последствия. Работа крупнейшей трубопроводной системы США была остановлена на пять дней, что привело к сбоям в поставках топлива на Восточное побережье страны. Это вызвало панику среди потребителей, дефицит на автозаправках и резкий рост цен на бензин. Президент США был вынужден объявить чрезвычайное положение. Атака нанесла значительный ущерб экономике и энергетической безопасности страны.

3. Какие меры должны предпринять компания для устранения последствий подобной кибератаки?

Ответ: Для устранения последствий кибератаки компания должна была: 1) провести расследование инцидента, чтобы оценить ущерб и выявить уязвимости в системах безопасности, 2) восстановить данные и системы, поврежденные в результате атаки, 3) уведомить пострадавших сотрудников и клиентов о произошедшем инциденте и предпринять меры для защиты их данных, 4) сотрудничать с правоохранительными органами и экспертами по кибербезопасности для расследования атаки и привлечения виновных к ответственности.

4. Какие меры по обеспечению кибербезопасности должны быть приняты для защиты своих информационных систем?

Ответ: Для защиты информационных систем от подобных атак компаниям необходимо внедрять комплексные меры по обеспечению кибербезопасности, включая: внедрение строгих политик управления доступом и использования паролей, регулярное обновление программного обеспечения и систем безопасности, использование многофакторной аутентификации для доступа к критически важным системам, шифрование данных в состоянии покоя и при передаче, резервное копирование данных и планы восстановления после аварий, обучение сотрудников по вопросам кибербезопасности и тестирование их готовности, сотрудничество с отраслевыми ассоциациями и правоохранительными органами для обмена информацией об угрозах.

5. Почему важны пароли и Какие существуют правила надежного пароля?

Ответ: Пароли являются ключевым элементом аутентификации и защиты доступа к системам и данным, поэтому важно соблюдать правила надежного пароля. Правила надежного пароля включают создание паролей длиной не менее 12 символов, состоящих из комбинации букв верхнего и нижнего регистра, цифр и специальных символов. Необходимо избегать использования очевидных слов, дат рождения и личных данных. Также важно не использовать один и тот же пароль для разных учетных записей и регулярно менять пароли, особенно если есть подозрение на их компрометацию. Рекомендуется использовать двухфакторную аутентификацию для дополнительной защиты. Способу хранения паролей также стоит уделять отдельное внимание: он должен храниться в надежном месте или в специально защищенных приложениях. Соблюдение этих правил значительно повышает защиту от взлома и кражи учетных данных, что показывает пример атаки на Colonial Pipeline. Надежные пароли в сочетании с многофакторной аутентификацией являются эффективным барьером для злоумышленников.

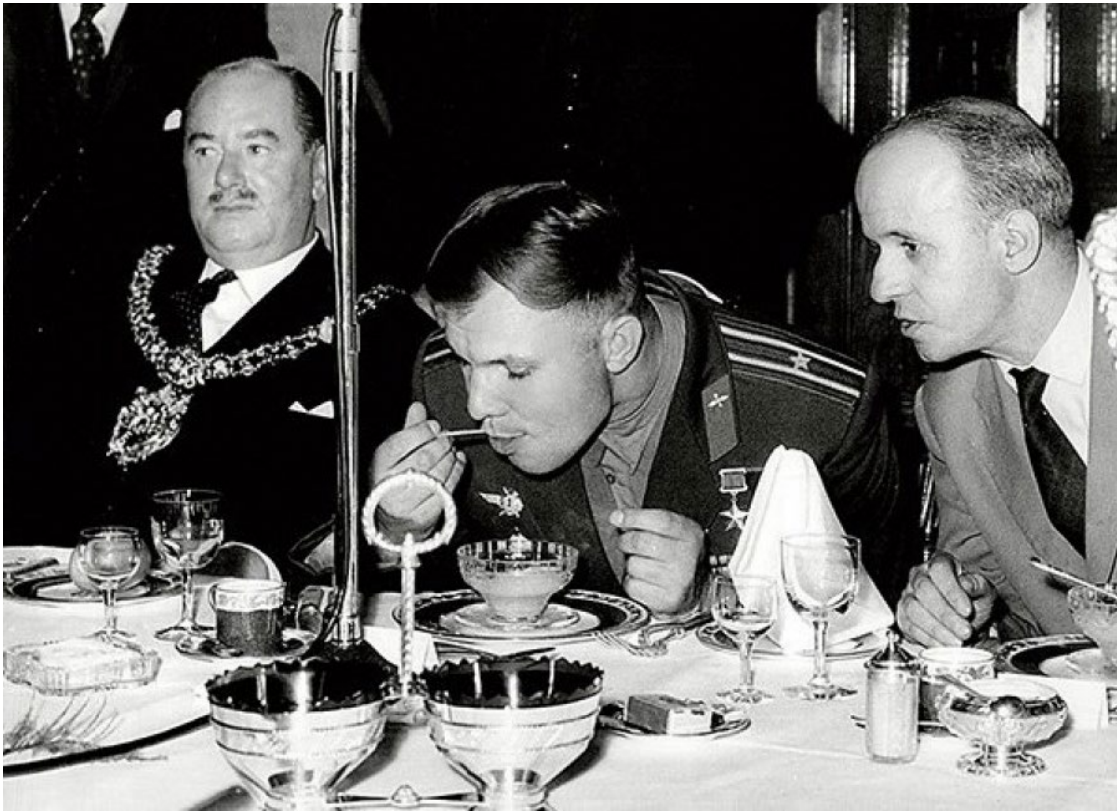
Задание 2.

Ознакомьтесь с фрагментом текста

Дворцовый этикет: вести себя за столом по-русски

В июле 1961 года первый в мире космонавт Гагарин посетил Великобританию, где был приглашён на приём к королеве Елизавете II. После завершения формальных протокольных мероприятий состоялся обед. Когда Гагарин увидел перед собой массу столовых приборов, на некоторое время растерялся, не зная, чем и как пользоваться.

Выручила его сама Елизавета II: увидев, что советский космонавт ступешевался, она спросила, что случилось. И тот откровенно признался — мол, не знаю, как пользоваться всем этим «инвентарём». На это монаршая особа спокойно ответила: «Знаете, хоть я здесь и живу всю жизнь, но сама до конца не знаю точно, для чего и какой столовый прибор нужен. Вы не стесняйтесь, официанты вам всё подскажут».



Вопрос: Правильно ли поступил советский космонавт, признавшись в слабом знании норм и правил поведения за столом?

Ответ: Юрий Алексеевич поступил совершенно правильно. В таких ситуациях существует два способа поведения: либо смотреть, как едят другие (но не американцы или итальянцы. – *В. В.*), либо действовать по подсказке официантов (ничего зазорного в этом нет). Он последовал рекомендации Елизаветы II, выбрав второе, и благодаря этому избежал очевидного нарушения норм и правил дворцового этикета.