Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Дипломатическая академия Министерства иностранных дел
Российской Федерации»
(ФГБОУ ВО «Дипломатическая академия МИД России»)

Методические рекомендации по решению кейсов Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» по направлению «Основы государственной безопасности и внешней политики (Международные отношения – МИД)»

Дисциплины:

Международные отношения, дипломатия

Темы элективных курсов:
Основы информационной безопасности,
Внешняя политика и дипломатия Российской Федерации

Москва
2024 год

Составители: Винокуров Владимир Иванович, доктор исторических наук, профессор Кафедры дипломатии и консульской службы Дипломатической академии МИД России;
Мартиросян Аревик Жораевна, научный сотрудник Института актуальных международных проблем Дипломатической академии МИД России.

Ответственные редакторы: Попова Наталья Николаевна, начальник Управления по развитию инновационных молодежных программ и профориентации Дипломатической академии МИД России;
Смирнова Анастасия Сергеевна, начальник отдела по содействию трудоустройству и связям с выпускниками Управления по развитию инновационных молодежных программ и профориентации Дипломатической академии МИД России.

1. Пояснительная записка

Данные методические рекомендации по решению кейсов практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» в номинации «Кадетский класс» по направлению «Основы государственной безопасности и внешней политики (Международные отношения – МИД)» (далее – Конкурс) предназначены для учителей с целью подготовки обучающихся дипломатических кадетских классов в рамках образовательного проекта «Кадетский класс в московской школе» к Конкурсу.

Конкурс проводится Московским центром качества образования в партнерстве с профильными федеральными вузами, участвующими в проектах предпрофессионального образования, в целях содействия развитию кадетских классов в общеобразовательных организациях города Москвы как элемента системы профильного обучения в условиях интеграции общего и дополнительного образования.

Проведение конкурса позволяет обеспечить независимую оценку качества подготовки обучающихся 11-х классов, освоивших программу предпрофессионального образования. Прохождение предпрофессиональной подготовки и последующее участие в Конкурсе способствуют осознанному выбору профессии и образовательной организации высшего образования для дальнейшего обучения по программам бакалавриата.

Теоретический этап Конкурса проходит на базе Московского центра качества образования и дает возможность обучающемуся набрать 60 баллов.

Практический этап Конкурса проводится на базе Дипломатической академии МИД России и оценивается максимум в 60 баллов.

Интеграционный характер предпрофессиональной подготовки в сфере международных отношений и дипломатии позволяет использовать знания школьных курсов истории, обществознания и дополнительных программ дипломатической направленности для подготовки к Конкурсу, что даст возможность школьникам расширить свои знания о будущей профессии

и скорректировать пробелы в знаниях, необходимых для успешного поступления в профильный вуз.

В рамках подготовки к Конкурсу обучающиеся знакомятся со следующими сферами международных отношений:

– основами информационной безопасности;

– внешней политикой и дипломатией Российской Федерации.

Знания и навыки, полученные в ходе участия в Конкурсе, будут полезны обучающимся дипломатических кадетских классов для понимания развития международных отношений в современных условиях, будут способствовать развитию эмоционального интеллекта, более трепетному отношению к Родине, к роли России в мире, осознанному выбору будущей профессии.

По итогам успешного участия в Конкурсе победители, набравшие от 100 до 120 баллов, получат 4 дополнительных балла при поступлении в Дипломатическую академию МИД России на все направления бакалавриата. Призеры, набравшие от 80 до 99 баллов, получат 3 дополнительных балла при поступлении в Дипломатическую академию МИД России на все направления бакалавриата.

В данном методическом пособии содержатся рекомендации по решению кейсов в рамках Конкурса, литература для подготовки, описание возможных трудностей, которые могут возникнуть в ходе решения кейсов.

2. Порядок проведения Конкурса

Конкурс позволяет проверить знания, полученные школьниками при изучении профильных предметов, и дает возможность продемонстрировать на практике умения, навыки и компетенции при выполнении кейсовых заданий.

На выполнение заданий практического этапа Конкурса отводится 60 минут. Во время проведения мероприятия участник может выйти из зоны проведения мероприятия не более чем на 5 минут, предупредив ответственного от вуза. Мероприятие не продлевается на время отсутствия участника. В течение первых 40 минут участники получают конкурсный вариант, знакомятся с ним и готовят ответы на поставленные вопросы. Ответ может быть сформулирован как письменно - на листе с конкурсным вариантом или черновике - так и в устной форме. В течение оставшихся 20 минут участники устно отвечают экспертам на вопросы конкурсного варианта.

Оценка ответа происходит на основе устного ответа, записи не проверяются. Задание считается выполненным, если ответ участника совпал с эталоном. Задание базового уровня сложности оцениваются в 24 балла, задание повышенного уровня – в 36 баллов. Максимальный балл за выполнение всех заданий – 60 баллов. Для получения максимального балла за практический этап Конкурса необходимо дать верные ответы на все задания.

Задания практического этапа Конкурса разработаны преподавателями Дипломатической академии МИД России, участвующей в проекте «Кадетский класс в московской школе».

Индивидуальный вариант участника формируется автоматически во время проведения практического этапа Конкурса предпрофессиональных умений из базы конкурсных заданий.

Индивидуальный вариант участника включает 2 задания, базирующихся на содержании элективных курсов по направлениям: «Основы информационной безопасности», «Внешняя политика и дипломатия Российской Федерации».

Конкурс проводится в очном формате.

Конкурсная комиссия, сформированная из представителей

профессорско-преподавательского состава вуза, проводит индивидуальную беседу с каждым участником по содержанию представленного им решения кейсов.

Результаты участников вносятся в итоговый протокол Конкурса, который подписывается председателем и всеми экспертами конкурсной комиссии. Далее протокол передаётся ответственному секретарю, и результаты публикуются в системе Московского центра качества образования.

3. Кейсы по темам элективных курсов

3.1. Основы информационной безопасности

3.1.1. Обзор решения демонстрационного кейса

Ознакомьтесь с фрагментом текста

В 2017 г. крупнейшая датская судоходная компания Maersk, работающая на международном рынке, столкнулась с серьезной кибератакой, которая произошла в результате недостаточной защиты ее информационных систем. Судоходная компания Maersk осуществляет перевозки между различными странами по всему миру, включая маршруты между Азией и Европой, трансатлантические маршруты между Северной Америкой и Европой, маршруты между Южной Америкой и Европой, а также Африкой, кроме того, внутренние маршруты в рамках отдельных регионов через свои дочерние компании MCC Transport и Seago Line. В целом, Maersk обслуживает 374 порта в 116 странах, что делает ее одной из крупнейших судоходных компаний в мире, способной обеспечивать глобальные логистические решения для своих клиентов, и ее системы управления флотом и логистикой хранят большое количество конфиденциальной информации о клиентах и грузах.

Хакеры отправили фальшивое электронное письмо, содержащее вредоносный файл, сотрудникам Maersk. Письмо выглядело как важное сообщение от делового партнера, что повысило вероятность его открытия. Когда один из сотрудников Maersk открыл вложение, вирус NotPetya был активирован. Он быстро распространился по сети компании, используя уязвимости в системах и инструментах безопасности. Вирус шифровал данные и блокировал доступ к критически важным системам компании, включая системы управления контейнерами и бухгалтерские системы. В результате это привело к полной остановке операций Maersk - суда не могли загружаться или разгружаться, терминалы были недоступны, а системы связи отключены. Доступ к основным системам был заблокирован. Злоумышленники внедрили вредоносный код в систему, что привело к сбоям в работе, и данные о грузах стали недоступны. На экране компьютеров появилось сообщение от хакеров, требующих выкуп в биткойнах за восстановление доступа к данным.

«Днем 27 июня 2017 г. озадаченные сотрудники начали по два-три

человека собираться возле стола, почти каждый из них держал ноутбук. На экранах устройств были надписи, сделанные черными и красными буквами. Одни надписи гласили «Восстановление системы файлов на диске C:» и настоятельно предупреждали не выключать компьютер. На других экранах было написано «Упс, ваши важные файлы засекречены» и требование заплатить за расшифровку сумму, эквивалентную 300$ в биткоинах».

Компания уведомила правоохранительные органы и начала внутреннее расследование. Компания также обратилась к международным экспертам по кибербезопасности для оценки ущерба и восстановления системы. В ходе расследования выяснилось, что кибератака была осуществлена через фишинговые письма, отправленные нескольким сотрудникам компании. Эти письма содержали вредоносные файлы, которые, будучи открытыми, позволили злоумышленникам получить доступ к учетным данным сотрудников и внутренним системам.

Восстановление заняло несколько недель. Примерно через две недели после атаки сеть Maersk смогла вновь выдать персональные компьютеры большинству сотрудников. Для полного устранения последствий пришлось заново выстраивать всю корпоративную информационную систему. В результате инцидента компания понесла значительные финансовые потери из-за простоя судов и необходимости восстановления данных: атака обошлась датской логистической компании Moller-Maersk в 200–300 миллионов долларов. Это стало одним из самых разрушительных инцидентов в истории кибербезопасности и продемонстрировало уязвимость крупных компаний к киберугрозам. Кроме того, репутация компании была подорвана, и некоторые клиенты начали искать альтернативные варианты для перевозки грузов.

Для предотвращения подобных инцидентов в будущем судоходная компания Maersk приняла ряд мер для улучшения своей кибербезопасности.

Вопросы к тексту:

1. Какова была основная причина кибератаки на судоходную компанию Maersk?

Ответ: Основной причиной кибератаки на судоходную компанию Maersk стало использование фишинговых писем, которые были отправлены

нескольким сотрудникам. Эти письма содержали вредоносные файлы, что позволило злоумышленникам получить доступ к внутренним системам компании и заблокировать доступ к важным данным.

2. Какие последствия имела компания в результате кибератаки?

Ответ: В результате кибератаки компания Maersk понесла значительные финансовые потери из-за простоя судов и необходимости восстановления данных. Также была подорвана репутация компании, что привело к потере клиентов, которые начали искать альтернативные варианты для перевозки грузов.

3. Какие меры необходимо принять для устранения последствий подобной кибератаки?

Ответ: Основные меры включают:

1. Уведомление правоохранительных органов, сотрудничество с отраслевыми ассоциациями для обмена информацией об угрозах.
2. Проведение внутреннего расследования.
3. Восстановление доступа к системам.
4. Внедрение многоуровневой аутентификации и новых протоколов для обработки электронной почты. Для повышения безопасности доступа к системам Maersk внедрила многоуровневую аутентификацию, что усложнило бы злоумышленникам доступ к учетным записям сотрудников
5. Обновление программного обеспечения. Maersk перешла на более современные версии операционной системы, включая Windows 10, чтобы устранить уязвимости, которые могли быть использованы злоумышленниками. Многие серверы, которые до атаки работали на устаревших версиях Windows, также были обновлены.
6. Улучшение резервного копирования. Компания усилила свои процедуры резервного копирования, чтобы обеспечить возможность быстрого восстановления данных в случае будущих атак.
7. Повышение киберграмотности сотрудников. Maersk начала проводить более интенсивное обучение сотрудников по вопросам кибербезопасности, включая распознавание фишинговых атак и других угроз.

8. Проведение постоянных аудитов безопасности. Компания начала регулярно проводить аудиты своей кибербезопасности, чтобы выявлять и устранять потенциальные уязвимости.

4. Какое значение имеет обучение сотрудников по вопросам кибербезопасности для судоходных компаний?

Ответ: Обучение сотрудников по вопросам кибербезопасности имеет критическое значение для судоходных компаний, так как сотрудники являются первой линией защиты от кибератак. Знания о том, как распознавать фишинговые письма и следовать протоколам безопасности, помогают снизить риски утечек данных и обеспечивают безопасность операций компании.

5. Как обнаружить фишинг и что делать в случае обнаружения?

Ответ: Обнаружить фишинг можно внимательно анализируя электронные письма и сообщения. Первое, на что стоит обратить внимание, - это адрес отправителя. Часто фишинговые письма приходят с адресов, которые выглядят подозрительно или немного отличаются от официальных. Также стоит обратить внимание на наличие ошибок в тексте, таких как опечатки или неправильная грамматика, поскольку многие фишинговые сообщения не проходят тщательной проверки. Кроме того, если письмо вызывает чувство срочности и требует немедленных действий, это может быть признаком фишинга. Не стоит переходить по ссылкам или открывать вложения, если вы не уверены в их безопасности. Лучше всего навести курсор на ссылку, чтобы увидеть, куда она ведет, прежде чем кликнуть.

При обнаружении фишинга важно не взаимодействовать с таким сообщением, уведомить службу поддержки платформы о подозрительном письме, чтобы они могли принять необходимые меры, удалить фишинговое сообщение из почтового ящика, чтобы избежать случайного открытия.

В случае, если учетные данные были введены на фальшивом сайте, необходимо немедленно изменить пароли.

3.1.2. Цели и задачи кейса

Цель: повышение киберграмостности школьников и формирование понимания современных технологий обеспечения информационной безопасности.

Задачи: получение общих знаний по информационной безопасности на примере реальных киберинцидентов и формирование у них необходимых знаний и навыков для безопасного и ответственного использования цифровых технологий.

3.1.3. Рекомендуемая литература

1. Роскомнадзор, официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Режим доступа: http://rkn.gov.ru/.

2. Цветкова М. С., Голубчиков С. В., Новиков В. К., Семибратов А. М., Якушина Е. В. Информационная безопасность: Правовые основы информационной безопасности. 10–11 классы: учебное пособие. — М.: БИНОМ. Лаборатория знаний, 2020. — 112 с.

3. Макаренко С. И. Информационная безопасность: учебное пособие. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил. Режим доступа: https://sccs.intelgr.com/editors/Makarenko/Makarenko-ib.pdf.

4. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск: Издательский центр ЮУрГУ, 2014. – 137 с. Режим доступа: https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000540003&dtype=F&etype=.pdf.

3.1.4. Список контролируемых требований к проверяемым умениям:

- осознание важности защиты информации и ее роли в современном обществе;

- знание основных понятий и терминов в области информационной безопасности;

- обретение системных знаний об угрозах и уязвимостях в области информационной безопасности;

- способность непрерывно совершенствовать киберграмотность и осознанно относиться к поведению в сети.

3.1.5. Навыки и знания для проверки в ходе решения кейса:

- знание основных понятий в области информационной безопасности, угроз и уязвимостей, методов защиты информации;

- умение собирать и обобщать информационный материал, работать с официальными документами, учебными и научными материалами, материалами СМИ по заданным темам, делать обоснованные выводы и на их основе принимать решения;

- умение применить на практике полученные навыки в области информационной безопасности;

- умение демонстрировать свои знания по программе дисциплины.

3.1.6. Контрольные вопросы для самопроверки и подготовки

1. Понятия приватности и конфиденциальности в контексте онлайн-взаимодействий.
2. Риски, связанные с публикацией личной информации в сети.
3. Основные правила безопасного поведения при публикации информации.
4. Утечки конфиденциальной информации: понятие, виды и предотвращение.
5. Конфиденциальная и чувствительная информация: понятие и способы защиты.
6. Определение фишинга и его основные разновидности (email-фишинг, SMS-фишинг и др.).
7. Основные законы и стандарты, регулирующие защиту информации в России.
8. Определение технических средств защиты информации и их роль в обеспечении информационной безопасности.
9. Информационные системы: уязвимости и защита.

3.1.7. Дополнительные рекомендации

Информационная безопасность – это область знаний, которая изучает методы и средства защиты информации от несанкционированного доступа, модификации, утечки или уничтожения. Она включает в себя комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности информации.

Она выступает неотъемлемым элементом современного образовательного процесса в цифровую эпоху, где информация и информационные технологии играют ключевую роль во всех сферах жизни общества. Информационная безопасность как междисциплинарная область знаний обеспечивает защиту информационных ресурсов и систем от различных угроз.

Изучение этой дисциплины в контексте международных отношений позволяет приобрести необходимые компетенции для понимания геополитических процессов с учетом особенностей ИКТ-среды. В эпоху глобализации и цифровизации страны сталкиваются с новыми угрозами, исходящими от новых технологий, которые требуют тесного международного сотрудничества, разработки совместных стратегий защиты и установления международных норм поведения в ИКТ-среде. Основы информационной безопасности закладывают базовое понимание основных направлений сотрудничества и глобальных угроз, требующих решения со стороны всего мирового сообщества.

3.2. Внешняя политика и дипломатия Российской Федерации

3.2.1. Обзор решения демонстрационного кейса

Ознакомьтесь с фрагментом текста

Историки утверждают, что событиям свойственно повторяться, но уже на новом витке исторической спирали, в новых условиях и обстоятельствах. И такое повторение из 1980-х гг.: США и их союзники предлагают человечеству в области контроля ракет средней и меньшей дальности (РСМД). Тогда решение США о переброске таких ракет в Европу, принятое глубокой осенью 1985 года, называлось «двойным». Согласно «первому решению» ракеты размещались вблизи границ СССР, «второе решение» заключалось в принуждении советского руководства к ограничению количества своих ракет средней и меньшей дальности.

В ответ с помощью РСД-10 «Пионер» Советский Союз взял под прицел фактически весь Старый Свет, разместив ракеты в странах Восточной Европы.

Это было опасно для обеих сторон, и в результате длительных и изнурительных дипломатических переговоров СССР и США 8 декабря 1987 года впервые в истории договорились полностью ликвидировать все комплексы баллистических и крылатых ракет наземного базирования средней (1000—5500 км) и меньшей (от 500 до 1000 км) дальности, а также не производить, не испытывать и не развёртывать такие ракеты в будущем. Это соглашение вошло в историю как Договор между СССР и США о ликвидации ракет средней и меньшей дальности (ДРСМД).

Договор просуществовал недолго: после нескольких взаимных обвинений в нарушении ДРСМД стороны в феврале 2019 года заявили о приостановлении соблюдения своих обязательств по нему, а 2 августа 2019 года Договор окончательно прекратил свое действие. Тем самым был нанесён удар по действовавшей до тех пор системе контроля над вооружениями, и мировое сообщество оказалось в ситуации риска полного распада этой системы.

И вот теперь эта история повторяется: 10 июля 2024 года правительства ФРГ и США выпустили совместное заявление, согласно которому США в 2026 году начнут развертывание в Германии ракет Tomahawk и SM-6, способных

достигать территории Урала. Эти планы некоторые находчивые журналисты назвали «двойным решением» 2.0.

МИД Российской Федерации еще в мае 2024 года заявлял о том, что Вашингтон размещает по всему миру наземные комплексы РСМД, имея в виду, что США и их союзники производят и испытывают данные типы вооружений. 28 июня 2024 года президент РФ Владимир Путин заявил о необходимости в ответ на действия США с системами РСМД и их размещению за пределами своих границ начать производство ракет средней и меньшей дальности в России.

Вопросы к тексту:

1. Что стоит за решением американской стороны повторить историю с РСМД 1980-х годов?

2. Какие действия нужно предпринять, чтобы США и ФРГ услышали Россию и отменили своё решение?

Ответы:

1. Американская сторона по-прежнему живёт в мире иллюзий превосходства США в сфере обладания самой большой сдерживающей военной силой, не желая признавать превосходство России по ряду современных вооружений и, прежде всего, в сфере гиперзвукового оружия. Стремление к сохранению глобального доминирования существенно ограничивает военно-политическое руководство США в двусторонних отношениях с РФ и не способствует поддержанию диалога с российской стороной по проблеме стратегической стабильности.

2. Не стоит ждать 2026 года, пока противник вооружит ФРГ и получит перевес. Нужно отвечать ассиметрично: в первую очередь необходимо настойчиво и целеустремленно с задействованием всех сил и средств дипломатии доводить до стран-участниц НАТО решимость России пересмотреть положения военной доктрины, касающиеся применения ядерного оружия, что с учётом высокой плотности населения европейских государств приведет к значительному увеличению их уязвимости.

3.2.2. Цели и задачи кейса

Цель: ознакомление обучающихся с действующей международной обстановкой и текущей внешней политикой и дипломатией Российской Федерации.

Задачи: достижение осознания обучающимися сложности складывающейся международной ситуации в области обеспечения национальных интересов и национальной безопасности России; уточнение основных целей и установок российской внешнеполитической доктрины; уяснение государственных структур и механизма принятия и реализации внешнеполитических решений в РФ.

3.2.3. Рекомендуемая литература

1. Алексеева Т. А., Казанцев А. А. Внешнеполитический процесс. Сравнительный анализ: Учеб. пособие. Гриф УМО. - М.: Аспект Пресс, 2012.

2. Ачкасов, В. А., Ланцов С.А. Мировая политика и международные отношения: Учебник. Гриф УМО. - М.: Аспект Пресс, 2011.

3. Винокуров В. И. Современная дипломатическая система: теория и практика: Учебник. М.: Русская панорама, 2022.

4. Винокуров В. И. Внешняя политика и дипломатия Российской Федерации: Учебное пособие для 10-11-х классов, Дипломатическая академия МИД России, 2023.

5. Лебедева М. М. Мировая политика (учебник). – М.: КноРус, 2013.

3.2.4. Список контролируемых требований к проверяемым умениям:

- способность системно мыслить, к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения;

- навыки поиска, сбора и первичного обобщения фактического материала и способность делать на его основе обоснованные выводы;

- понимание важности постоянного отслеживания международных событий и их анализа по «горячим следам»;

- готовность к работе в составе коллектива. проявить свои лидерские качества и принять на себя ответственность;

- умение логически верно, аргументированно и ясно строить устную и письменную речь.

3.2.5. Навыки и знания для проверки в ходе решения кейса:

- знание основных целей и положений российской внешнеполитической доктрины, а также государственных структур и механизма принятия и реализации внешнеполитических решений в РФ;

- знакомство с особенностями складывающейся международной обстановки и вытекающих из неё последствий для государственной безопасности нашей страны;

- стремление к саморазвитию, повышению своей квалификации и мастерства;

- настрой на развитие креативности, профессиональности, инициацию позитивных перемен.

3.2.6. Контрольные вопросы для самопроверки и подготовки

1. Государственные структуры - участники внешнеполитической деятельности в Российской Федерации.
2. Механизм принятия и реализации внешнеполитический решений и стадии его функционирования.
3. Содержание внешнеполитической доктрины и её нормативно-правовая база.
4. Организация и проведение переговоров на высоком и высшем уровнях.
5. Контроль вооружений – разоружение или забота о мире.
6. Особенности ведения переговоров на треке стратегических, оперативных и тактических вооружений.
7. Переговоры как важное средство мирного урегулирования конфликтов.
8. Дипломатические иммунитеты и привилегии и их роль в жизни и деятельности дипломата.
9. Роль и место дипломатического протокола и этикета в международном общении.

3.2.7. Дополнительные рекомендации

Дипломатию называют искусством переговоров, которые, в свою очередь, являются одним из главных средств мирного разрешения международных споров и конфликтов. Роль и значение дипломатии и переговоров особенно востребованы ныне в сложных условиях международной обстановки,

поскольку альтернативой им становится применение военной силы, что сопряжено с риском возникновения ядерной войны. Сегодня, как никогда в прошлом, выросла задача овладеть наукой сотрудничества государств во имя мира. А эта наука проявляется прежде всего в умении вести равноправный диалог в сфере стратегической стабильности и контроля над вооружениями.

Трудности, которые могут возникнуть:

1. Американцы всегда были уверены в своем военном преимуществе перед нашей страной и не учитывают того, что переговоры с Россией можно вести только на равноправной и взаимовыгодной основе.
2. На протяжении всего послевоенного времени США пытаются использовать сотрудничество в области контроля над вооружениями для извлечения собственных выгод. Это им удалось, в частности, при заключении Договора о ракетах средней и меньшей дальности (РСМД) 8 декабря 1987 года, в результате которого Советский Союз уничтожил гораздо больше ракет, чем это сделали США.
3. В результате выхода США из Договора по ПРО, Договора по РСМД и Договора по открытому небу на современном этапе отсутствует какой-либо эффективный контроль над гонкой вооружений.