Спецификация конкурсных материалов для проведения практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» в номинации «Кадетский класс» для направления «Основы государственной безопасности и внешней политики (Международные отношения – МИД)»

1. Назначение конкурсных материалов

Материалы практического этапа Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» (далее – Конкурс) предназначены для оценки уровня практической подготовки участников Конкурса.

2. Условия проведения

Практический этап Конкурса проводится в очной форме на базе вуза. При выполнении работы обеспечивается строгое соблюдение порядка организации и проведения Конкурса.

3. Продолжительность выполнения

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.

4. Содержание и структура

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

5. Система оценивания

Задание считается выполненным, если ответ участника совпал с эталоном. Максимальный балл за выполнение всех заданий – 60 баллов.

6. Приложения

1. План конкурсных материалов для проведения практического этапа Конкурса.
2. Демонстрационный вариант конкурсных заданий практического этапа Конкурса.

Приложение 1

План конкурсных материалов для проведения *практического* этапа Конкурса

№ задания	Уровень сложности	Уникальные кодификаторы Конкурса	Контролируемые требования к проверяемым умениям	Балл
1.	*Базов*ый	Понятие «информационной безопасности» и ее виды	**Знать:** Теоретические основы информационной безопасности: сущность и особенности. **Уметь:** Анализировать различные аспекты информационной безопасности и их взаимосвязи.	24
		Понятие «угрозы информационной безопасности» и ее виды	**Знать:** Определение угроз информационной безопасности и их влияние на личную и общественную жизнь. **Уметь:** Давать характеристики видам угроз информационной безопасности и приводить примеры.	
		Технические средства защиты информации и основные каналы утечки	**Знать:** Определение технических средств защиты информации и их роль в обеспечении информационной безопасности. Разновидности каналов утечки информации. **Владеть навыками:** Использовать технические средства защиты информации и способность распознавать потенциальные каналы утечки информации и принимать меры предосторожности.	
		Защита информационных систем. Основные методы и средства	**Знать:** Основы защиты информационных систем: определение, методы, средства. **Уметь:** Применять методы защиты информационных систем, анализировать и оценивать уровень защиты информационных систем	

		Публикация персональной информации. Приватность и конфиденци-альность в сети	**Знать:** Понятия приватности и конфиденциальности в контексте онлайн-взаимодействий. Значение приватности и конфиденциальности в Интернете. Риски, связанные с публикацией личной информации в сети. Основные правила безопасного поведения при публикации информации. **Уметь:** Оценивать, какую информацию безопасно публиковать в Интернете. Настраивать параметры конфиденциальности в социальных сетях и других онлайн-сервисах. Идентифицировать потенциальные угрозы, связанные с публикацией личной информации. **Владеть:** Умением анализировать риски, связанные с публикацией информации. Способностью принимать обоснованные решения о том, какой информацией делиться в сети. Навыками работы с настройками конфиденциальности на различных платформах.	
		Фишинг. Варианты воздействия и способы защиты. Социальная инженерия. Правила безопасности при общении в сети. Безопасность аккаунтов в сети. Совершение покупок онлайн.	**Знать:** Определение фишинга и его основные разновидности (email-фишинг, SMS-фишинг и др.). Принципы социальной инженерии и методы манипуляции. Основные правила безопасности при общении в Интернете. Способы защиты аккаунтов и безопасные методы совершения покупок онлайн. **Уметь:** Распознавать фишинговые сообщения и сайты. Применять правила безопасности при общении в сети и совершении покупок. Настраивать двухфакторную аутентификацию	

			и использовать надежные пароли для защиты аккаунтов. **Владеть:** Умением критически оценивать информацию и сообщения, получаемые в сети. Способностью применять правила безопасности в повседневной жизни. Навыками защиты своих аккаунтов и личной информации в Интернете.	
		Основные нормативные руководящие документы Российской Федерации в области информационной безопасности	**Знать:** Значение нормативных документов в области информационной безопасности. Основные законы и стандарты, регулирующие защиту информации в России. Права и обязанности граждан в области информационной безопасности. **Уметь:** Находить и использовать нормативные документы, касающиеся информационной безопасности. Анализировать требования законодательства и применять их на практике. **Владеть:** Умением работать с юридическими документами и извлекать из них необходимую информацию. Способностью понимать и интерпретировать законодательные нормы в области информационной безопасности. Навыками критического мышления и анализа информации из нормативных источников.	
2.	*Повышенный*	Подходы России к решению глобальных проблем современности (транснациональные вызовы и угрозы)	**Знать:** Основные цели и положения российской внешнеполитической доктрины, а также государственную структуру и механизмы принятия и реализации внешнеполитических решений в РФ. Отдельные детали в области контроля над вооружениями.	36

			Складывающуюся международную обстановку. **Уметь:** Системно мыслить, обобщать, анализировать, воспринимать информацию, ставить цели и выбирать пути ее достижения. Логично и аргументированно излагать свою позицию. Логически верно, аргументированно и ясно строить устную и письменную речь. **Владеть**: Навыками поиска, сбора и первичного обобщения фактического материала и способностью делать на его основе обоснованные выводы.	
				Сумма баллов: **60**

Приложение 2

Демонстрационный вариант конкурсных заданий практического этапа Конкурса

Пример состава задания практического этапа Конкурса

ЗАДАНИЕ 1.

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.

Критерии оценки

24-26 баллов	Систематическое и глубокое знание программного материала по дисциплине. При работе с кейсом применил навыки синтеза и анализа с использованием междисциплинарных знаний; правильно и развернуто аргументировал свою позицию по ответу; выдвинутые положения иллюстрированы примерами; использовал специальную терминологию по дисциплине; высказал свою точку зрения. Разница между 26 и 24 баллами - в подаче материала.
21-23 балла	Ответ полный и правильный (на основании изученного материала). Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен литературным языком в определенной логической последовательности, осознанно с использованием современных научных терминов; ответ самостоятельный. Обучающийся уверенно отвечает на дополнительные вопросы. Умеет свободно ориентироваться в теме. Разница между 23 и 21 баллами - в подаче материала.

18-20 баллов	Правильно и развернуто аргументировал свою позицию по ответу; выдвинутые положения иллюстрированы примерами; использовал терминологию по дисциплине. При работе с кейсом применил навыки синтеза и анализа с использованием междисциплинарных знаний; свою точку зрения высказал, но уверенности в ответе не было. Разница между 20 и 18 баллами - в подаче материала.
15-17 баллов	Правильно и развернуто аргументировал свою позицию по ответу; однако выдвинутые положения не иллюстрировал примерами; использовал специальную терминологию по дисциплине, хотя не всегда. Применил навыки обобщения и анализа, однако не в полном объеме. Умело использовал информацию из смежных дисциплин. Свою точку зрения не высказал. Показал в целом хорошие знания по дисциплине. Разница между 17 и 15 баллами - в подаче материала.
12-14 баллов	В целом продемонстрировал систематические знания программного материала по предмету, однако ответ был неполным, поскольку пытался уйти в сторону и «заменить» материалом по другим вопросам. Продемонстрировал интерес к изучаемому предмету, но без привлечения дополнительной литературы. Ответ по заданному кейсу был недостаточно аргументирован. Не показал знаний в использовании специальной терминологии. Разница между 14 и 12 баллами - в подаче материала.
9-11 баллов	В целом продемонстрировал определенные знания программного материала по предмету, однако ответ был неполным, поскольку пытался уйти в сторону и «заменить» материалом по другим вопросам. Продемонстрировал интерес к изучаемому предмету, но без привлечения дополнительной литературы. Ответ по заданному кейсу был недостаточно аргументирован. Не ответил на дополнительные вопросы. Разница между 11 и 9 баллами - в подаче материала.
6-8 баллов	Ответ по заданному кейсу не дает четкого представления о сформулированных знаниях и компетенциях изучаемого предмета. Испытывает трудности при формулировках и выстраивании логики ответа. Не использовал терминологию по дисциплине; не продемонстрировал навыки обобщения и анализа информации с использованием междисциплинарных знаний. В целом обнаруживается недостаточное раскрытие теоретического материала.

	Разница между 8 и 6 баллами - в подаче материала.
3-5 баллов	Имеет слабые представления о дисциплине, однако предпринял попытку в решении кейса; испытывает некоторые трудности в ответах на вопросы.
0-2 балла	Имеет слабые представления о дисциплине или отказался отвечать.

ЗАДАНИЕ 2.

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 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 области 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.

Критерии оценки

29–36 баллов	- Дал объективную оценку рассматриваемой проблеме; - правильно определил цель задания, выбрал оптимальный путь его решения и сформулировал логически правильные выводы; - использовал навыки обобщения и анализа информации с учетом междисциплинарных знаний и положений; - проявил самостоятельность, последовательность и оригинальность; - продемонстрировал культуру мышления, логическое изложение проблемы, проведение анализа задачи; - использовал ссылки на научную и учебную литературу.
18–28 баллов	- Смог дать объективную оценку рассмотренной проблеме; - проявил самостоятельность; - проявил логичность в изложении проблемы; - использовал навыки анализа информации с использованием междисциплинарных знаний и положений; - поставил в целом правильную цель, но выбрал ошибочные пути ее оптимального достижения; - не смог сформулировать конкретные выводы; - не использовал ссылки на научную и учебную литературу.
10–17 баллов	- Смог отчасти дать оценку рассмотренной проблеме; - поставил ошибочную цель и неправильно выбрал пути ее достижения; - проявил определенную самостоятельность; - применил некоторую логичность в изложении проблемы; - не в полной мере использовал навыки анализа информации с использованием междисциплинарных знаний и положений; - не смог сформулировать конкретные выводы; - не использовал ссылки на научную и учебную литературу.
0–9 баллов	- Неубедительно высказал свою точку зрения или не высказал ее вообще; - не проявил свои способности логично мыслить и делать правильные выводы.

ПРОЦЕДУРА ПРОВЕДЕНИЯ ПРАКТИЧЕСКОГО ЭТАПА КОНКУРСА

Практический этап Московского конкурса межпредметных навыков и знаний «Интеллектуальный мегаполис. Потенциал» в номинации «Кадетский класс» для направления «Основы государственной безопасности и внешней политики (Международные отношения – МИД)» рассчитан на 60 минут. 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 голове участника. В течение оставшихся 20 минут участники устно отвечают экспертам на вопросы конкурсного варианта. Оценка ответа происходит на основе устного ответа, записи не проверяются. В конце участники оставляют конкурсные варианты и далее ожидают появления результатов в личных кабинетах на портале МЦКО.