

**Совет Безопасности**

Distr.: General  
10 June 2024  
Russian  
Original: English

---

**Письмо Постоянного представителя Республики Корея  
при Организации Объединенных Наций от 7 июня 2024 года  
на имя Председателя Совета Безопасности**

Имею честь настоящим препроводить пригласительное письмо и концептуальную записку для открытых прений высокого уровня Совета Безопасности на тему «Поддержание международного мира и безопасности: противодействие меняющимся угрозам в киберпространстве», которые состоятся в четверг, 20 июня 2024 года, в 10 ч 00 мин (см. приложение).

Буду признателен Вам за распространение настоящего письма и приложения к нему в качестве документа Совета Безопасности.

*(Подпись)* Джун Гук Хван  
Посол и Постоянный представитель  
Республики Корея при Организации Объединенных Наций



## **Приложение к письму Постоянного представителя Республики Корея при Организации Объединенных Наций от 7 июня 2024 года на имя Председателя Совета Безопасности**

Имею честь пригласить вас на открытые дебаты высокого уровня Совета Безопасности на тему «Поддержание международного мира и безопасности: противодействие меняющимся угрозам в киберпространстве», которые состоятся в четверг, 20 июня, в 10 ч 00 мин в зале Совета Безопасности (см. концептуальную записку). Они станут знаковым мероприятием, которое Республика Корея проведет в качестве Председателя Совета Безопасности в июне.

На фоне стремительного развития информационно-коммуникационных технологий, которое имеет свои преимущества и вместе с тем чревато проблемами в условиях нашего гиперсвязанного мира, изошренная и оказывающая глубокое воздействие злонамеренная деятельность с использованием киберсредств вызывает серьезную обеспокоенность в контексте международного мира и безопасности. В этой связи меняющаяся ситуация в области безопасности в киберпространстве требует от Совета пристального внимания к киберугрозам, которые могут затронуть все страны.

Открытые дебаты высокого уровня пройдут под председательством министра иностранных дел Республики Корея Чхо Дэ Юля и станут ценной возможностью для Совета выполнить свою главную обязанность по поддержанию международного мира и безопасности в эпоху, когда киберугрозы приобретают все большие масштабы. Участие представителей высокого уровня в этом мероприятии позволит значительно повысить содержательность прений.

*(Подпись)* Джун Гук Хван  
Постоянный представитель

**Концептуальная записка для открытых прений высокого уровня Совета Безопасности на тему «Поддержание международного мира и безопасности: противодействие меняющимся угрозам в киберпространстве», 20 июня 2024 года, 10 ч 00 мин**

**Справочная информация**

Развитие информационно-коммуникационных технологий (ИКТ) приносит огромные плоды в экономической, социальной, культурной, гражданской и политической сферах, однако, учитывая высокую степень зависимости от цифровой инфраструктуры в области связи, торговли и управления, злонамеренная деятельность в киберпространстве может пошатнуть международный мир и безопасность, затронув одновременно несколько сфер.

Злонамеренная деятельность с использованием киберсредств, затрагивающая критически важную инфраструктуру, включая больницы и другие учреждения системы здравоохранения, финансовые услуги, энергетический сектор, спутники, транспорт и другие системы, обеспечивающие чрезвычайное реагирование, становится все более распространенным явлением. Такая деятельность может иметь разрушительные последствия для национальной безопасности и порождать значительный риск причинения вреда гражданскому населению. Помимо распространения злонамеренной деятельности, усугубление ситуации с угрозами связано с применением меняющихся и совершенствуемых методов, включая использование вирусов-вымогателей в качестве прикрытия, применение модели «программа-вымогатель как услуга» и кражи криптовалюты для содействия террористической деятельности и для финансирования программ создания ядерного оружия и другого оружия массового уничтожения; ситуация дополнительно осложняется появлением новых векторов атаки и факторов уязвимости, которые могут быть использованы.

Хотя злонамеренная деятельность с использованием киберсредств ведется в самых разных обстоятельствах, особую тревогу вызывает использование этих технологий в связи с вооруженными конфликтами и в целях содействия ведению таких конфликтов. Злонамеренная деятельность с использованием киберсредств может как усугублять существующие конфликтные ситуации, так и способствовать возникновению новых очагов напряженности.

Учитывая транснациональный характер киберпространства, ни одно государство не застраховано от вреда, связанного со злонамеренной деятельностью с использованием киберсредств. Мощность сети кибербезопасности определяется прочностью ее самого слабого звена. В этой связи неотъемлемым элементом сотрудничества между всеми соответствующими форумами, которые занимаются вопросами, связанными с ИКТ, в рамках системы Организации Объединенных Наций, является наращивание потенциала. Различия в потенциале или в степени киберустойчивости создают дополнительные проблемы в плане выявления злонамеренной деятельности с использованием киберсредств, защиты от нее и принятия соответствующих мер реагирования, особенно для тех государств, которые не обладают достаточным потенциалом. Вредоносное использование ИКТ может оказывать несоразмерно сильное воздействие на определенные группы населения, включая женщин и меньшинства.

## Роль Совета Безопасности

### *Ход работы*

За последнее десятилетие Совет Безопасности все больше внимания уделяет воздействию вопросов, связанных с киберпространством, на международный мир и безопасность. С 2016 года Совет провел несколько заседаний по формуле Аррии, в ходе которых государства рассматривали вопросы кибербезопасности в контексте различных взаимосвязей с такими темами, как защита критически важной инфраструктуры, защита гражданского населения и дезинформация и язык ненависти в киберпространстве. Эстония провела первые открытые прения высокого уровня по этой теме в 2021 году, что способствовало дополнительному закреплению вопроса о поддержании международного мира и безопасности в киберпространстве в качестве одной из тем для рассмотрения Советом.

Последнее из состоявшихся заседаний по формуле Аррии, посвященное вопросам кибербезопасности, было организовано Республикой Корея и проведено совместно с США и Японией в апреле 2024 года. На заседании было особо отмечено растущее воздействие киберугроз в контексте международного мира и безопасности, а также значимая роль Совета Безопасности в снижении напряженности и обеспечении кибербезопасности.

### *Возможные варианты действий*

Крайне важной и своевременной задачей является выработка государствами общей позиции и усиление роли Совета Безопасности в противодействии киберугрозам. Активное участие Совета в обеспечении кибербезопасности в соответствии с его главной обязанностью по поддержанию международного мира и безопасности позволяет ему реагировать на злонамеренную деятельность с использованием киберсредств и тем самым вносить существенный вклад в создание безопасного, открытого и мирного киберпространства в глобальном масштабе в интересах всех стран.

Такое участие Совета Безопасности может приобретать формы, дополняющие собой другие текущие процессы в области ИКТ в Организации Объединенных Наций, включая соответствующие обсуждения норм ответственного поведения государств в сфере использования ИКТ и рамочной основы Организации Объединенных Наций, касающейся ответственного поведения государств в сфере использования информационно-коммуникационных технологий и принятой на основе консенсуса под эгидой Генеральной Ассамблеи.

На заседании по формуле Аррии, состоявшемся в апреле, были предложены возможные варианты действий для рассмотрения Советом Безопасности с целью повысить эффективность различных многосторонних усилий по решению проблем, связанных с последствиями злонамеренной деятельности с использованием киберсредств для международного мира и безопасности.

Например, Совет Безопасности мог бы рассмотреть вопрос о проведении — предпочтительно на регулярной основе — брифинга для обзора меняющейся ситуации в плане киберугроз в связи с действующим мандатом и повесткой дня Совета. Разработка оценок и стратегий в связи с меняющейся ситуацией с киберугрозами на основе учета всеобъемлющей информации, получаемой от структур системы Организации Объединенных Наций, частного сектора, гражданского общества и научных кругов, позволит Совету оставаться в курсе новых событий и их последствий для международного мира и безопасности.

С учетом того, что угрозы международному миру и безопасности, исходящие из киберпространства, по сути своей носят межсекторальный характер, Совет Безопасности мог бы также изучить возможности для обеспечения всестороннего учета проблем, связанных с киберпространством или ИКТ, при обсуждении страновых дозье или других тематических дозье, таких как миссии по поддержанию мира и миростроительству, вводимые Советом санкции, женщины и мир и безопасность или нераспространение и противодействие терроризму. Помимо этого, в работу по каждому из этих направлений деятельности могут быть интегрированы усилия по повышению киберустойчивости, укреплению национального потенциала для обеспечения кибербезопасности и развитию международного сотрудничества.

Кроме того, государства — члены Организации Объединенных Наций могли бы изучить возможности укрепления потенциала Совета Безопасности для реагирования на злонамеренное использование ИКТ, представляющее угрозу международному миру и безопасности, особенно связанную с защитой гражданского населения, критически важной инфраструктурой и гуманитарными усилиями, и обеспечения более целостного подхода к поддержанию мира и безопасности.

### **Ориентировочные вопросы**

Нижеперечисленные вопросы могут послужить ориентиром при подготовке выступлений государств-членов:

- В чем состоят основные возникающие и развивающиеся тенденции злонамеренной деятельности в киберпространстве, создающей угрозу международному миру и безопасности?
- В чем проявляется воздействие злонамеренного использования ИКТ как «мультипликатора угроз» в контексте существующих конфликтов и проблем, требующее участия Совета Безопасности?
- Какие конкретные функции и действия может выполнить Совет Безопасности для решения проблем для международного мира и безопасности, исходящих из киберпространства, и какое развитие могут получить эти функции в рамках его мандата и на взаимоукрепляющей и взаимодополняющей основе с усилиями, предпринимаемым другими органами Организации Объединенных Наций? Какие дальнейшие меры необходимо принять?
- Как киберугрозы взаимосвязаны с другими пунктами повестки дня Совета Безопасности? Каким образом Совет Безопасности может эффективно обеспечить всесторонний учет проблем, связанных с киберпространством и ИКТ, в своей текущей работе?

### **Формат и докладчики**

Открытые прения высокого уровня будут проходить под председательством министра иностранных дел Республики Корея Чхо Дэ Юля, и членам Совета предлагается принять участие в прениях на уровне министров. Чтобы могли выступить как можно больше представителей государств-членов, продолжительность выступлений будет ограничена тремя минутами.

Перед Советом Безопасности выступят следующие докладчики:

- Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш

- Стефан Дюген, главный административный сотрудник, институт «Кибер-Мир»
- Нненна Ифеани-Аджуфо, профессор права и технологий, Лидский университет им. Беккета, Соединенное Королевство

Запись в список ораторов, желающих выступить на открытых прениях, откроется 17 июня, за три рабочих дня до заседания, в 9 ч 30 мин. Для записи в модуль eSpeakers портала e-deleGATE должно быть загружено письмо на имя Председателя Совета Безопасности, должным образом подписанное постоянным представителем или временным поверенным в делах, с просьбой об участии на основании правила 37 временных правил процедуры Совета.

---