Организация Объединенных Наций A/77/88/Add.1

Генеральная Ассамблея

Distr.: General
7 June 2022
Russian
Original: English

Семьдесят седьмая сессия
Пункт 145 первоначального перечня*
Объединенная инспекционная группа

Обзор положения в сфере кибербезопасности в организациях системы Организации Объединенных Наций

Записка Генерального секретаря

Генеральный секретарь имеет честь препроводить членам Генеральной Ассамблеи свои замечания, а также замечания Координационного совета руководителей системы Организации Объединенных Наций по докладу Объединенной инспекционной группы, озаглавленному «Кибербезопасность в организациях Организации Объединенных Наций» (см. A/77/88).

* A/77/50.

I. Введение

1. В докладе Объединенной инспекционной группы под названием «Кибербезопасность в организациях системы Организации Объединенных Наций» (см. A/77/88) представлен обзор положения в сфере кибербезопасности в организациях системы Организации Объединенных Наций, выполненные прежде всего с целью: a) выявить и проанализировать общие проблемы и риски кибербезопасности, с которыми сталкиваются организации системы Организации Объединенных Наций по отдельности, а также принимаемые этими организациями меры реагирования на них с учетом конкретных требований организаций (вертикальная перспектива); и b) изучить нынешнюю межучрежденческую динамику, способствующую общесистемному подходу к обеспечению кибербезопасности для улучшения координации, взаимодействия и обмена информацией между организациями системы Организации Объединенных Наций, а при необходимости и возможность выработки общих решений (горизонтальная перспектива).

II. Общие замечания

2. Организации с удовлетворением отмечают этот доклад и содержащиеся в нем выводы, которые могут помочь усилить кибербезопасность в системе Организации Объединенных Наций. Они также с удовлетворением отмечают, что в этом обзоре акцентируются: a) необходимость применения подхода, основанного на учете организационных рисков, вместо более традиционного подхода, сфокусированного на информационно-коммуникационных технологиях (ИКТ); b) внутриорганизационный взгляд/процессы; и c) настоятельная необходимость обеспечения общего и совместного базового уровня защиты/мер безопасности в рамках всей системы Организации Объединенных Наций для преодоления разницы в уровне зрелости между организациями и повышения киберустойчивости всей системы Организации Объединенных Наций.

3. Организации поддерживают сделанные по итогам обзора рекомендации.

III. Замечания по конкретным рекомендациям

Рекомендация 1
Исполнительным главам организаций системы Организации Объединенных Наций следует в первоочередном порядке и не позднее 2022 года подготовить всеобъемлющий доклад о своей системе кибербезопасности и представить его своим соответствующим директивным и руководящим органам при первой возможности, охватив элементы, способствующие повышению киберустойчивости, рассмотренной в настоящем докладе.

4. Организации поддерживают эту рекомендацию.

5. Не исключено, что в некоторых структурах регулярно представляемая управленческая отчетность по вопросам кибербезопасности уже отвечает потребностям, в связи с которыми была вынесена данная рекомендация: например, отчетность, представляемая руководящим органам, комитетам по ревизии и надзору или внутренним советам по информационным технологиям на уровне организации и внешним экспертным консультативным советам по технологиям.

6. Организации подчеркивают, что при подготовке докладов, которые рекомендуется представлять, важно — учитывая, что это открытые документы, — не

раскрывать деталей, подтверждающих конкретную информацию об обнаружении атак и возможностях обнаружения в соответствующих организациях, и не предоставлять информации, которую потенциальный противник мог бы использовать для повышения вероятности успешного осуществления конкретных атак.

Рекомендация 2
Директивным и руководящим органам организаций системы Организации Объединенных Наций следует по мере необходимости рассматривать подготовленные исполнительными главами доклады об элементах, способствующих повышению киберустойчивости, и давать стратегические указания относительно дальнейших улучшений, которые должны быть достигнуты в их организациях.

7. Организации отмечают, что эта рекомендация адресована их директивным и руководящим органам.

8. В запрошенных стратегических указаниях необходимо учитывать, что для укрепления местных средств обеспечения кибербезопасности и содействия сотрудничеству с Международным вычислительным центром Организации Объединенных Наций (МВЦ) потребуются дополнительные ресурсы.

Рекомендация 3
Директору Международного вычислительного центра Организации Объединенных Наций следует стремиться к созданию не позднее конца 2022 года целевого фонда донорских взносов, который дополнил бы возможности Центра по проектированию, разработке и предложению общих услуг и решений для улучшения состояния кибербезопасности в организациях системы Организации Объединенных Наций.

9. Организации отмечают, что эта рекомендация адресована директору МВЦ.

10. Дополнительные и специализированные совместные услуги, которые разработает МВЦ, могут быть полезны небольшим организациям, которым недостает ресурсов и специалистов в сфере кибербезопасности. Структуры, которые реализуют программы развития цифровых технологий и гуманитарные программы через государственно-частные партнерства, хотели бы продолжать получать прямую поддержку от государств-членов в осуществлении своих цифровых программ, в том числе в вопросах кибербезопасности, и в связи с этим некоторые из них трактуют эту рекомендацию как распространяющуюся на внутреннюю кибербезопасность их отделений повсюду в мире и кибербезопасность/факторы риски, связанные с внешней работой с государственно-частными партнерами.

11. Некоторые организации — члены МВЦ отмечают, что, если эта рекомендация будет выполняться, то до окончательной доработки соответствующего предложения они хотели бы сказать свое слово в ходе обсуждения вопросов, касающихся управления этим целевым фондом, его финансирования, его работы и доступа к нему, в том числе на основе контактов с Сетью по вопросам цифровизации и технологий.

Рекомендация 4
Генеральной Ассамблее Организации Объединенных Наций следует не позднее чем на своей семьдесят седьмой сессии принять к сведению рекомендацию, адресованную директору Международного вычислительного центра Организации Объединенных Наций, о создании целевого фонда для совместных решений по кибербезопасности и предложить государствам-членам, желающим улучшить состояние кибербезопасности в организациях системы Организации Объединенных Наций, сделать взносы в целевой фонд.

12. Структуры отмечают, что эта рекомендация адресована Генеральной Ассамблее, и повторяют комментарии, представленные в ответ на рекомендацию 3.

Рекомендация 5
Генеральному секретарю следует представить Генеральной Ассамблее Организации Объединенных Наций не позднее ее семьдесят восьмой сессии доклад об изучении дальнейших возможностей использования сближения физической безопасности и кибербезопасности в целях обеспечения более комплексной защиты персонала и ресурсов Организации Объединенных Наций, определяющий необходимые меры по соответствующему укреплению имеющихся структур, с уделением особого внимания возможной роли Департамента охраны и безопасности в этой связи.

13. Организации отмечают, что эта рекомендация адресована Генеральному секретарю.

14. Секретариат Организации Объединенных Наций уже инициировал такой процесс. Помимо того, что Управление информационно-коммуникационных технологий и Департамент охраны и безопасности сотрудничают на неформальной и единовременной основе, Департамент также входит в недавно созданную сеть реагирования на гибридные кибератаки. Кроме того, в рамках плана капитальных вложений для операций в сфере ИКТ будет рассмотрен вопрос об инвестициях, необходимых для укрепления существующих структур, кадрового потенциала, активов и услуг с целью извлечь пользу из сближения физической безопасности и кибербезопасности.

15. Что касается согласования функций физической безопасности и кибербезопасности, то некоторые организации усматривают в формулировке пункта 164 доклада. Хотя инспекторы признают, что функции обеспечения кибербезопасности не следует поручать тому же подразделению, которое занимается вопросами физической безопасности, они тем не менее рекомендуют сблизить эти функции, что может создать в различных учреждениях такую ситуацию, которая приведет к тому самому результату, который инспекторы считают нежелательным. Эти организации предлагают особо отметить, что функции кибербезопасности не должны быть поглощены подразделениями, которые обеспечивают физическую безопасность.

16. Несмотря на текущее сотрудничество по вопросам кибербезопасности между Департаментом и Управлением, следует отметить, что ведущую роль в этом отношении будет играть Управление и что роль и ресурсы Департамента будут ограничены обеспечением физической безопасности персонала и помещений Организации Объединенных Наций, поскольку кибербезопасность не входит в его компетенцию. Это партнерство активизируется в случае гибридных кибератак [1] на Организацию Объединенных Наций, когда Департамент и

[1] В данном контексте под гибридной кибератакой понимается использование цифровых технологий или физическое нападение на инфраструктуру информационных технологий

Управление совместно проводят оценки рисков безопасности и готовят и выполняют рекомендации, касающиеся превентивных мер и мер по уменьшению последствий.

для нанесения преднамеренного ущерба программам и деятельности Организации Объединенных Наций, приводящее к значительной уязвимости физической безопасности в помещениях Организации Объединенных Наций или повышенному риску причинения вреда сотрудникам.