

РЕЗОЛЮЦИЯ 69 (Пересм. Баку, 2025 г.)

Содействие созданию и совершенствованию национальных групп реагирования на компьютерные инциденты, в частности в развивающихся странах, и сотрудничеству между ними

Всемирная конференция по развитию электросвязи (Баку, 2025 г.),

напоминая

- a)* о Резолюциях 101, 102 и 130 (Пересм. Бухарест, 2022 г.) Полномочной конференции, в которых подчеркивается необходимость сотрудничества;
- b)* о Резолюции 58 (Пересм. Нью-Дели, 2024 г.) Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) о поощрении создания и совершенствования национальных групп реагирования на компьютерные инциденты (CIRT), в частности для развивающихся стран¹;
- c)* о Резолюции 50 (Пересм. Нью-Дели, 2024 г.) ВАСЭ о кибербезопасности;
- d)* о Резолюции 214 (Бухарест, 2022 г.) Полномочной конференции о технологиях искусственного интеллекта (ИИ) и электросвязи/информационно-коммуникационных технологиях (ИКТ), в рамках которой Директор Бюро развития электросвязи (БРЭ) может поддерживать работу Сектора развития электросвязи (МСЭ-D) по решению проблем и использованию возможностей, которые открывает ИИ как одна из новых и появляющихся технологий применительно к национальным CIRT при реагировании на инциденты в области кибербезопасности,

признавая

- a)* рост уровня использования компьютеров и степени зависимости использования ИКТ от наличия компьютеров в развивающихся странах;

¹ К ним относятся наименее развитые страны, малые островные развивающиеся государства, развивающиеся страны, не имеющие выхода к морю, и страны с переходной экономикой.

- b) подверженность развивающихся стран угрозам кибербезопасности и кибератакам, направленным на их сети ИКТ, а также возможность лучшей подготовки к таким инцидентам в сфере кибербезопасности и повышенному уровню мошеннических действий с применением этих средств;
- c) необходимость укрепления сотрудничества и потенциала для реагирования на связанные с кибербезопасностью проблемы;
- d) результаты работы по исследуемому Вопросу 3/2, проделанной до настоящего времени 2-й Исследовательской комиссией МСЭ-D, и отчеты по этой теме, которые включают поддержку создания и координации групп CIRT и создание партнерств государственного и частного секторов;
- e) работу, проделанную до настоящего времени БРЭ по объединению усилий Государств-Членов и других заинтересованных сторон в целях содействия странам в создании национального потенциала по управлению инцидентами, такого как группы CIRT;
- f) важность обеспечения должной степени готовности к чрезвычайным ситуациям в области кибербезопасности во всех странах, в частности в развивающихся странах, путем создания групп CIRT на национальной основе, важность координации усилий внутри регионов и между ними и использования преимуществ региональных и международных инициатив в этой области, включая сотрудничество МСЭ с региональными и глобальными проектами и организациями, такими как, среди прочего, Форум групп реагирования на инциденты и обеспечения безопасности (FIRST), Организация американских государств и Группа реагирования на нарушение компьютерной защиты Азиатско-Тихоокеанского региона;
- g) что появляющиеся технологии электросвязи/ИКТ применяются как часть технических мер против кибератак и угроз в сфере кибербезопасности;
- h) соответствующую работу 17-й Исследовательской комиссии Сектора стандартизации электросвязи МСЭ (МСЭ-T), в том числе по методам обмена информацией о кибербезопасности;
- i) что странам может быть полезно осуществлять координацию между национальными секторальными CIRT, если таковые существуют, для совершенствования управления инцидентами во время крупных инцидентов в сфере кибербезопасности, имеющих внутригосударственные межсекторальные последствия;
- j) результаты деятельности МСЭ-D, связанной с оценкой, планированием, созданием, совершенствованием и сотрудничеством национальных групп CIRT,

отмечая,

- a)* что в развивающихся странах повысился, но по-прежнему сохраняется низкий уровень готовности к реагированию на нарушения в области кибербезопасности;
- b)* что высокий уровень взаимосвязанности сетей на базе электросвязи/ИКТ может быть нарушен вследствие кибератак и угроз в сфере кибербезопасности, исходящих из сетей менее подготовленных к обеспечению защиты стран, каковыми в большинстве случаев являются развивающиеся страны;
- c)* что страны могут столкнуться со значительными новыми проблемами и возможностями при реагировании на инциденты в области кибербезопасности по мере продолжающегося развития новых и появляющихся услуг и технологий электросвязи/ИКТ;
- d)* пункт *i)* раздела *учитывая* Резолюции 130 (Пересм. Бухарест, 2022 г.), в котором указано, что для защиты таких инфраструктур, решения этих проблем и противодействия этим угрозам требуются скоординированные действия на национальном, региональном и международном уровнях, направленные на предотвращение, подготовку, а также реагирование в связи с тем или иным инцидентом с компьютерной безопасностью и на восстановление после него со стороны органов государственного управления на национальном (включая создание групп CIRT) и субнациональном уровнях, со стороны частного сектора, граждан и пользователей, в дополнение к международному и региональному сотрудничеству и координации, и что МСЭ должен играть ведущую роль в этой области в соответствии со своим мандатом и компетенцией;
- e)* что учреждение и совершенствование CIRT требует постоянного выделения надлежащих ресурсов для обеспечения их эффективности и устойчивости;
- f)* работу 17-й Исследовательской комиссии МСЭ-Т, касающуюся национальных групп CIRT, в частности для развивающихся стран, и сотрудничества между ними, которая отражена в намеченных результатах деятельности этой исследовательской комиссии;
- g)* необходимость учреждения в соответствующих случаях групп CIRT на национальной основе, в том числе групп CIRT, ответственных за межправительственное сотрудничество, и важность координации усилий всех соответствующих организаций;
- h)* Глобальную программу кибербезопасности МСЭ (ГПК) и Руководящие указания по использованию МСЭ ГПК, утвержденные Советом МСЭ;

i) расширение использования новых и появляющихся технологий электросвязи/ИКТ во всех аспектах жизни, включая цифровизацию государственных услуг, которым необходима высокая степень защиты;

j) что CIRT могут помочь удовлетворить насущную потребность в повышении безопасности и укреплении уверенности и доверия при использовании ИКТ,

решает

1 содействовать созданию и совершенствованию национальных групп CIRT в Государствах-Членах, которым требуется поддержка, в зависимости от обстоятельств, в рамках имеющихся ресурсов бюджета;

2 содействовать тому, чтобы МСЭ-D продолжал свою работу, связанную с оценкой, планированием, созданием, совершенствованием и сотрудничеством национальных групп CIRT,

порукает Директору Бюро развития электросвязи

1 пропагандировать национальный, региональный и международный передовой опыт по созданию и совершенствованию групп CIRT и Центров анализа и обмена информацией (ISAC), определенный к настоящему времени соответствующими исследовательскими комиссиями МСЭ, например 2-й Исследовательской комиссией МСЭ-D в рамках Вопроса 3/2 и 17-й Исследовательской комиссией МСЭ-T, а также другими соответствующими организациями и экспертами;

2 обеспечить развитие потенциала национальных групп CIRT, в особенности в области новых и появляющихся услуг и технологий электросвязи/ИКТ, через региональные и зональные отделения МСЭ, с учетом финансовых ресурсов, включая содействие проведению постоянной оценки уровня развития;

3 оказывать содействие национальным группам CIRT, особенно в развивающихся странах, путем обмена руководящими указаниями и передовым опытом, касающимися проблем и возможностей реагирования на инциденты в области кибербезопасности, которые возникают в результате использования новых и появляющихся услуг и технологий электросвязи/ИКТ;

4 обеспечить поддержку национальным группам CIRT в расширении обмена информацией, сотрудничества и обмена передовым опытом в целях реагирования на инциденты в сфере кибербезопасности для повышения уровня готовности к чрезвычайным ситуациям в области кибербезопасности, в особенности в развивающихся странах во всем мире;

5 содействовать созданию соответствующей эксплуатационной структуры CIRT в тех Государствах-Членах, в которых такие группы создаются, если это применимо;

6 продолжать мобилизацию ресурсов для содействия организации необходимых программ профессиональной подготовки в этой области, включая многоуровневые программы обучения (начального, среднего и продвинутого уровней), способствующие постепенному созданию потенциала, и продолжать предоставлять надлежащую поддержку тем развивающимся странам, которые хотят ее получить;

7 содействовать распространению передового опыта в области создания национальной структуры, способной координировать деятельность национальных секторальных групп CIRT, если таковые существуют, и совершенствовать управление инцидентами во время значительных инцидентов в сфере кибербезопасности, имеющих внутригосударственные межсекторальные последствия;

8 продолжать поощрять сотрудничество между национальными группами CIRT, в том числе группами CIRT, ответственными за межправительственное сотрудничество, группами CIRT отраслевых и академических организаций, осуществляемого в соответствии с национальным законодательством на региональном и глобальном уровнях путем поддержки участия развивающихся стран в региональных и глобальных проектах и в работе соответствующих организаций, таких как, в том числе, FIRST и региональные организации;

9 работать в направлении достижения этих целей, при этом избегая дублирования усилий с другими организациями;

10 продолжать разработку программ кампаний по повышению осведомленности о важности создания и совершенствования групп CIRT для повышения уровня обеспечения кибербезопасности;

11 продолжать совершенствовать существующие комплекты материалов, которые развивающиеся страны могли бы использовать для проведения теоретических или тренировочных занятий по реагированию на инциденты,

предлагает Государствам-Членам

1 создавать, в соответствующих случаях, национальные группы CIRT, в том числе группы CIRT, ответственные за межправительственное сотрудничество, где существует в них необходимость или где они в настоящее время отсутствуют;

2 повышать уровень развития, функциональные возможности и устойчивость созданных национальных групп CIRT для эффективного противодействия возникающим угрозам в сфере кибербезопасности;

3 вносить вклад в разработку платформы информационного ресурса на основании положений Решения 630 (C23) Совета, с тем чтобы создать и поддерживать хранилище примеров передового опыта по созданию и функционированию национальных CIRT;

4 тесно сотрудничать с МСЭ-D, МСЭ-T и другими соответствующими организациями, принимая во внимание Резолюцию 58 (Пересм. Нью-Дели, 2024 г.) в этом отношении, в зависимости от случая;

5 оказывать содействие и поддержку обмену передовым опытом между национальными группами CIRT, в том числе участвовать в соответствующих инициативах CIRT, таких как FIRST;

6 поощрять использование новых и появляющихся технологий электросвязи/ИКТ для расширения технических возможностей CIRT;

7 рассмотреть, при необходимости, возможность создания национальной структуры, способной осуществлять координацию между национальными секторальными CIRT, там, где они присутствуют, в целях повышения эффективности управления инцидентами во время крупных инцидентов в сфере кибербезопасности, имеющих внутригосударственные межсекторальные последствия;

8 поощрять на добровольной основе обмен информацией о факторах уязвимости и угрозах в сфере кибербезопасности между Государствами-Членами, в том числе через существующие платформы обмена информацией;

9 доводить свои потребности до сведения региональных и зональных отделений МСЭ,

предлагает Членам Сектора, Ассоциированным членам и Академическим организациям, в зависимости от обстоятельств,

1 вносить вклад в создание и совершенствование национальных групп CIRT, в частности для развивающихся стран;

2 поддерживать инициативы по созданию потенциала национальных CIRT в области новых и появляющихся услуг и технологий электросвязи/ИКТ, в частности для развивающихся стран;

3 вносить вклад в дискуссии, обмен информацией, создание потенциала и исследования, посвященные проблемам и возможностям, с которыми сталкиваются национальные группы CIRT при реагировании на инциденты в области кибербезопасности по мере дальнейшего развития и использования технологий ИИ в сфере электросвязи/ИКТ с целью повышения их эффективности и функциональности.