

Статья 2

Основные направления сотрудничества

1. С учетом основных угроз, указанных в статье 1 настоящего Соглашения, Стороны, уполномоченные представители и компетентные органы государств Сторон, которые определяются в соответствии со статьей 4 настоящего Соглашения, осуществляют сотрудничество в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий по следующим основным направлениям:
 - 1) определение, согласование и осуществление необходимого взаимодействия для обеспечения безопасности в сфере использования информационно-коммуникационных технологий;
 - 2) осуществление мониторинга возникающих угроз в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий и реагирование на них;
 - 3) разработка и продвижение норм международного права, а также правил, норм и принципов ответственного поведения государств в информационно-коммуникационной среде в целях обеспечения национальной и международной безопасности в сфере использования информационно-коммуникационных технологий;
 - 4) противодействие основным угрозам в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий, указанным в статье 1 настоящего Соглашения;
 - 5) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения безопасности в сфере использования информационно-коммуникационных технологий в целях обнаружения, предупреждения и ликвидации последствий ИКТ-инцидентов. Для целей настоящего Соглашения под ИКТ-инцидентом Стороны понимают факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;
 - 6) взаимодействие в правоохранительной сфере по предупреждению, выявлению, пресечению и расследованию правонарушений и преступлений, связанных с использованием информационно-коммуникационных технологий в террористических, экстремистских и иных преступных целях;
 - 7) разработка и осуществление необходимых совместных мер доверия, способствующих обеспечению безопасности в сфере использования информационно-коммуникационных технологий;
 - 8) обмен информацией о законодательстве каждого из государств Сторон по вопросам обеспечения безопасности в сфере использования информационно-коммуникационных технологий;
 - 9) содействие совершенствованию двусторонней нормативно-правовой базы и практических механизмов сотрудничества государств Сторон в обеспечении безопасности в сфере использования информационно-коммуникационных технологий;
 - 10) создание условий для взаимодействия компетентных органов государств Сторон в целях реализации настоящего Соглашения;
 - 11) углубление взаимодействия и координации деятельности государств Сторон по проблемам обеспечения безопасности в сфере использования информационно-коммуникационных технологий в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный союз электросвязи, Международную организацию по стандартизации, Международную организацию уголовной полиции - Интерпол и др.);
 - 12) содействие научным исследованиям в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

13) содействие в подготовке специалистов, обмене студентами, аспирантами и преподавателями профильных высших учебных заведений государств Сторон в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

14) проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов государств Сторон по тематике безопасности в сфере использования информационно-коммуникационных технологий.

2. Стороны или компетентные органы государств Сторон могут по взаимной договоренности определять другие направления сотрудничества.