Концепция Конвенции ООН об обеспечении международной информационной безопасности

ПРЕАМБУЛА

Отмечаем значительный прогресс в развитии информационно-коммуникационных технологий и средств, формирующих информационное пространство,

выражаем озабоченность угрозами, связанными с возможностями использования таких технологий и средств в целях, не совместимых с задачами обеспечения международного мира, безопасности и стратегической стабильности,

придаем важное значение предотвращению конфликтов в информационном пространстве и налаживанию эффективного взаимодействия в этой области в глобальном, региональном, многостороннем и двустороннем форматах, а также *отмечаем* в этом контексте резолюции Генеральной Ассамблеи Организации Объединенных Наций от 27 декабря 2013 г. A/RES/68/243, от 2 декабря 2014 г. A/RES/69/28, от 23 декабря 2015 г. A/RES/70/237, от 5 декабря 2016 г. A/RES/71/28, от 5 декабря 2018 г. A/RES/73/27, от 12 декабря 2019 г. A/RES/74/29 и от 31 декабря 2020 г. A/RES/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», способствующие прогрессу в этом вопросе,

придаем важное значение формированию системы международной информационной безопасности как одному из ключевых элементов системы международной безопасности в целом, направленному на обеспечение глобальной стабильности в условиях нарастающей зависимости информационного общества от информационно-коммуникационных технологий,

убеждены в том, что дальнейшее углубление доверия и развитие взаимодействия государств-участников в вопросах обеспечения международной информационной безопасности являются объективной необходимостью и отвечают их интересам,

принимаем во внимание важное значение информационной безопасности для реализации основных прав и свобод человека и гражданина, прежде всего права на уважение частной жизни и защиту персональных данных,

желаем создать правовые и организационные основы сотрудничества государств-участников в области обеспечения международной информационной безопасности,

ссылаемся на резолюцию Генеральной Ассамблеи Организации Объединенных Наций от 20 ноября 2000 г. A/RES/55/29 «Роль науки и техники в контексте международной безопасности и разоружения», в которой, в частности, признается, что достижения науки и техники могут иметь как

гражданское, так и военное применение, и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

признаем необходимость предотвращения угроз, связанных с использованием информационно-коммуникационных технологий в целях, не совместимых с обеспечением стратегической стабильности и международной информационной безопасности, и способных оказать отрицательное воздействие на целостность цифровых инфраструктур, нанося ущерб их безопасности,

подчеркиваем необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с противоправным использованием информационно-коммуникационных технологий в военно-политических, террористических и преступных целях,

отмечаем главенствующую роль Организации Объединенных Наций в процессе обеспечения информационной безопасности государств-участников и создания безопасного глобального информационного пространства, а также важное значение деятельности других международных и региональных организаций,

подчеркиваем важность формирования общего понимания и обеспечения международного сотрудничества на равноправной основе в интересах безопасного, непрерывного и стабильного функционирования сети «Интернет» и других информационно-коммуникационных сетей, их защищенности от возможных угроз,

подтверждаем, что политические полномочия по связанным с сетью «Интернет» вопросам являются суверенным правом государств, и что государства имеют права и обязанности в отношении решения таких вопросов на международном уровне,

отмечаем необходимость активизации усилий по преодолению «цифрового разрыва» путем обеспечения доступности информационно-коммуникационных технологий развивающимся странам и наращивания их потенциала в вопросах передовой практики и профессиональной подготовки в области обеспечения безопасности в сфере использования данных технологий,

убеждены в необходимости реализации государствами политики, нацеленной на защиту граждан от противоправных деяний в информационном пространстве, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества,

обеспокоены угрозой того, что информационнотелекоммуникационные сети, включая сеть «Интернет», могут также использоваться для совершения противоправных деяний, и *учитываем*, что в этих сетях сохраняются «цифровые» доказательства совершения таких деяний,

признаем необходимость сотрудничества между государствами и деловыми кругами в борьбе с противоправными деяниями в информационном

пространстве и необходимость защиты их законных интересов в сфере использования и развития информационно-коммуникационных технологий,

полагаем, что для эффективной борьбы с противоправными деяниями в информационном пространстве требуется более широкое, оперативное и хорошо отлаженное международное сотрудничество, и *отмечаем* в этом контексте резолюцию Генеральной Ассамблеи Организации Объединенных Наций от 27 декабря 2019 г. A/RES/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» и учреждение в соответствии с данной резолюцией специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях,

исходим из необходимости обеспечения должного баланса между предусмотренным Международным пактом о гражданских и политических правах 1966 года правом человека на свободное выражение своего мнения, включающим свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору, и предусмотренными данным Пактом особыми обязанностями и особой ответственностью, налагаемыми в связи с пользованием указанными правами, что может быть сопряжено с некоторыми ограничениями, установленными законом и являющимися необходимыми для уважения прав и репутации других лиц, а также для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения,

приветствуем стремление государств к дальнейшему наращиванию взаимопонимания, доверия и сотрудничества по обеспечению международной информационной безопасности, включая усилия, предпринимаемые Организацией Объединенных Наций, Шанхайской организацией сотрудничества, БРИКС, Содружеством Независимых Государств, Европейским союзом, Советом Европы, Организацией по безопасности и сотрудничеству в Европе, Организацией Азиатско-Тихоокеанского сотрудничества, Центральноамериканской интеграционной системой, Организацией американских государств, Ассоциацией стран Юго-Восточной Азии, Африканским союзом и другими международными организациями и форумами.

ОБЩИЕ ПОЛОЖЕНИЯ

Цели Конвенции

Содействие формированию системы международной информационной безопасности, обеспечивающей противодействие угрозам международному

миру, безопасности и стратегической стабильности в информационной сфере, а также способствующей:

а) равноправному стратегическому партнерству в глобальном информационном пространстве на основе суверенного равенства государств;

б) общему социальному и экономическому развитию на основе равноправного и безопасного доступа всех государств к достижениям современных ИКТ;

в) реализации общепризнанных принципов и норм международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека;

г) реализации права каждого искать, получать и распространять всякого рода информацию и идеи с учетом того, что такое право может быть сопряжено с ограничениями, установленными законом и являющимися необходимыми для уважения прав и репутации других лиц, а также для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения;

д) свободному технологическому обмену и свободному обмену информацией с учетом уважения суверенитета государств и их существующих политических, правовых, исторических и культурных особенностей.

Основные угрозы и факторы, влияющие на обеспечение международнойинформационной безопасности

1. Использование информационно-коммуникационных технологий в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

2. Использование информационно-коммуникационных технологий в террористических целях, в том числе для проведения компьютерных атак на объекты информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников.

3. Использование информационно-коммуникационных технологий для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию, а также для нанесения вреда общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

4. Использование информационно-коммуникационных технологий для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

5. Использование информационных ресурсов, находящихся под юрисдикцией другого государства, без согласования с компетентными структурами этого государства.

6. Распространение вредоносного программного обеспечения и информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств.

7. Использование информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационном пространстве, прежде всего праву человека на уважение его личной (частной) жизни.

8. Нарушение безопасного, непрерывного и стабильного функционирования сети «Интернет».

9. Противодействие доступу к новейшим информационно-коммуникационным технологиям, создание условий технологической зависимости в сфере информатизации.

10. Включение в информационно-коммуникационные технологии и средства недекларируемых возможностей, а также сокрытие производителями информации об уязвимостях в их продуктах.

11. Недостаточная оценка возникающих угроз информационной безопасности, связанных с внедрением новых технологий, таких как искусственный интеллект, «большие данные», интернет вещей, блокчейн и другие.

12. Использование технологического доминирования для монополизации различных сегментов рынка информационно-коммуникационных технологий, включая основные информационные ресурсы, критическую инфраструктуру, ключевые технологии, продукты и услуги, а также для препятствования осуществлению независимого контроля и проведению мероприятий, направленных на обеспечение информационной безопасности.

13. Допущение использования государствами своей информационной инфраструктуры для совершения международно-противоправных деяний, а также использование государствами посредников, в том числе негосударственных субъектов, для совершения таких деяний.

14. Публичное распространение под видом достоверных сообщений заведомо ложной информации, приводящее к возникновению угрозы жизни и безопасности граждан или к наступлению тяжких последствий.

15. Невозможность точной идентификации источника компьютерных атак или ложной информации, обусловленная технологическими особенностями информационно-коммуникационных технологий, а также отсутствием

организационных механизмов обеспечения деанонимизации информационного пространства.

Основные принципы обеспечения международной информационной безопасности

1. Совместимость с задачами поддержания международного мира, безопасности и стратегической стабильности.

2. Соответствие общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека.

3. Неделимость безопасности, означающая, что безопасность каждого государства неразрывно связана с безопасностью всех других государств и должна обеспечиваться без ущерба безопасности других государств.

4. Достаточность потенциала любого государства по обеспечению безопасности национального информационного пространства.

5. Суверенное равенство и одинаковые права, а также одинаковые обязанности государств независимо от различий экономического, социального, политического или иного характера.

6. Возможность установления суверенных норм и механизмов управления своим информационным пространством в соответствии с национальными законами.

7. Свобода и самостоятельность в реализации своих суверенных интересов в информационной сфере, а также свобода в выборе способов обеспечения собственной информационной безопасности в соответствии с международным правом.

8. Урегулирование конфликтов путем переговоров, посредничества, примирения, обращения к профильным региональным органам или иными мирными средствами по своему выбору таким образом, чтобы не подвергать угрозам международный мир и безопасность.

9. Применимость неотъемлемого права на самооборону перед лицом агрессивных действий в информационном пространстве при условии достоверного установления источника агрессии и адекватности ответных мер с учетом норм международного гуманитарного права.

10. Недопустимость бездоказательных и необоснованных обвинений других государств в совершении противоправных деяний с использованием информационно-коммуникационных технологий, включая компьютерные атаки, в том числе для последующего принятия различного рода наказаний в виде санкций и иных способов реагирования.

11. Соблюдение основных прав и свобод граждан, включая защиту от несанкционированного вмешательства в частную жизнь граждан, и соблюдение при этом баланса между этими правами и задачами противодействия использованию информационного пространства в террористических и иных преступных целях.

12. Недопустимость ограничений или нарушений доступа к информационному пространству кроме как в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

13. Недопустимость трансграничного доступа к компьютерной информации, хранящейся в информационной системе другого государства, без официального взаимодействия с правоохранительными органами данного государства.

14. Добровольность и взаимность в деятельности по предупреждению, выявлению, пресечению, раскрытию и расследованию противоправных деяний в сфере использования информационно-коммуникационных технологий, в том числе в террористических и иных преступных целях, и ликвидации последствий таких деяний.

ПРЕДОТВРАЩЕНИЕ КОНФЛИКТОВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Основные меры предотвращения конфликтов в информационном пространстве

1. Сотрудничество в сфере обеспечения международной информационной безопасности для поддержания международного мира и безопасности, а также международной экономической стабильности.

2. Создание государствами механизмов для предотвращения деструктивного информационного воздействия (проведения компьютерных атак) с их территории или с использованием информационной инфраструктуры, находящейся под их юрисдикцией, а также для взаимодействия в целях определения источника компьютерных атак, проведенных с их территории, противодействия этим атакам и ликвидации их последствий.

3. Воздержание от разработки и принятия доктринальных документов и планов, способных спровоцировать нарастание угроз и возникновение конфликтов в информационном пространстве, а также вызвать напряженность в отношениях между государствами.

4. Воздержание от любых действий, угрожающих безопасности информационного пространства другого государства.

5. Неиспользование информационно-коммуникационных технологий для вмешательства в дела, относящиеся к внутренней компетенции другого государства.

6. Воздержание от организации или поощрения организации каких-либо иррегулярных сил для осуществления противоправных деяний в информационном пространстве другого государства.

7. Противодействие распространению недостоверной или искаженной информации при соблюдении недискриминационного характера доступа к ресурсам.

8. Противодействие созданию, распространению и применению технологий и средств для осуществления противоправной деятельности с использованием информационно-коммуникационных технологий.

9. Противодействие разработке, распространению и использованию вредоносного программного обеспечения.

10. Воспрепятствование несанкционированному вмешательству в деятельность международных информационных систем управления транспортными и финансовыми потоками, средствами связи, средствами международного информационного, в том числе научного и образовательного, обмена.

11. Содействие разработке и использованию безопасных информационно-коммуникационных технологий с соблюдением принципа нейтральности глобальной сети связи, включая эволюционное реформирование протоколов и способов передачи информации для исключения возможности использования данной сети в противоправных целях.

12. Обеспечение защиты охраняемой законом информации, включая интеллектуальную собственность, торговые марки и авторские права.

13. Стимулирование государственно-частного партнерства в целях снижения угроз информационной безопасности и повышения уровня безопасности.

14. Обеспечение осведомленности граждан, общественных и государственных органов, профильных структур и международных организаций о новых угрозах в информационном пространстве и об известных путях их нейтрализации, а также повышение грамотности всех пользователей в сфере информационной безопасности.

ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ

Основные меры противодействия использованию информационного пространства в террористических целях

1. Координация действий для предотвращения любой террористической деятельности с использованием информационно-коммуникационных технологий.

2. Оперативный обмен информацией о признаках, фактах, методах и средствах использования информационного пространства в террористических целях, в том числе с помощью компьютерных атак, а также взаимное информирование о правовом регулировании и организации деятельности по борьбе с этими противоправными деяниями, о накопленном опыте и практике деятельности в данной сфере.

3. Совершенствование законодательства для организации деятельности правоохранительных и других органов по противодействию и пресечению использования информационного пространства в террористических целях.

ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

Уголовно наказуемые деяния в сфере использования информационно-коммуникационных технологий

1. Уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации.

2. Создание, использование или распространение вредоносных программ.

3. Нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия.

4. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации.

5. Распространение с использованием сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего.

6. Изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети.

7. Незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб.

8. Распространение с использованием сети «Интернет» материалов, признанных в установленном порядке экстремистскими или содержащих

призывы к осуществлению террористической деятельности или оправданию терроризма.

9. Распространение с использованием сети «Интернет» информации, содержащей сцены агрессии и насилия, а также информации, порочащей честь и достоинство личности.

10. Неправомерное воздействие на критическую информационную инфраструктуру.

Основные меры противодействия использованию информационно-коммуникационных технологий в преступных целях

1. Совершенствование договорно-правовой базы сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, включая соответствующие двусторонние и многосторонние международные договоры, в том числе о правовой помощи по уголовным делам, а также в рамках международного полицейского сотрудничества, включая каналы Международной организации уголовной полиции – Интерпола.

2. Разработка и реализация совместных программ и планов противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

3. Сотрудничество с профильными международными организациями по пресечению и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий.

4. Организация взаимодействия для выполнения положений международных нормативных правовых документов, направленных на борьбу с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий.

5. Оказание взаимной консультативной помощи в разработке национальной системы мер противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

6. Оказание содействия при осуществлении следственных действий, оперативно-разыскных и иных мероприятий по противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

7. Обмен опытом работы по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий, проведение совместных семинаров, учений, сборов, консультаций и совещаний.

8. Совершенствование методов и форм взаимодействия между компетентными органами в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, внедрение передового опыта в практику деятельности указанных органов.

9. Подготовка, переподготовка и повышение квалификации кадров, участвующих в противодействии преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

10. Проведение совместных научных исследований в области противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Обмен национальными концепциями обеспечения информационной безопасности (безопасности в сфере использования информационно-коммуникационных технологий).

2. Оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации.

3. Обмен информацией о компьютерных инцидентах и компьютерных атаках, совершенных в отношении государств, с учетом того, что объем такой информации будет определяться самими государствами.

4. Проведение консультаций по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность, в целях предотвращения и мирного урегулирования конфликтов в информационном пространстве.

5. Обмен информацией о мерах по обеспечению открытого, безопасного и стабильного функционирования сети «Интернет».

6. Развитие государственно-частного партнерства и механизмов обмена передовым опытом реагирования на угрозы международной информационной безопасности.

Источник: http://www.scrf.gov.ru/security/information/document112/