Доверие и безопасность в информационном обществе

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СОВРЕМЕННАЯ ПРОБЛЕМА

Статья рекомендована к публикации членом редакционного совета А.А. Стрельцовым 20.05.2022.

Прохорова Дарья Александровна

Московский государственный университет имени М.В. Ломоносова, Факультет глобальных процессов, магистр
Москва, Российская Федерация
dularno@yandex.ru

Аннотация

В статье рассматривается роль информации и информационно-коммуникационных технологий, которые являются не только символом современного общественного развития информационного общества, но и предвестником новых угроз международной безопасности. Проанализированы особенности понятий «защищенность», «информационная безопасность» и «международная информационная безопасность», роль ООН как ключевого международного координатора деятельности по обеспечению международной информационной безопасности, а также значение действующих в составе ООН специализированных организаций и рабочих групп, касающееся данной тематики. Обосновывается необходимость формирования и дальнейшего развития категориального аппарата, способствующего наиболее глубокому и полному изучению как проблем информатизации, так и проблем связанной с ней информационной безопасности.

Ключевые слова

международная информационная безопасность, ООН, комитет по информации, информация, безопасность, защищенность

Введение

Информационная сфера сегодня является системообразующим фактором общественной жизни, что делает её отличительным признаком современного глобального мира [23]. Нормальное функционирование государства серьезно зависит от того, насколько развита информационная инфраструктура в нем. Однако с точки зрения международных отношений информационные технологии стали не только средством развития и укрепления взаимодействия между глобальными акторами, но и орудием их противоборства. Об этом свидетельствует потрясшая мир в 2010 году кибератака на завод по обогащению урана в Натанзе, Иран, предположительно организованная США [39]. Вирус Stuxnet спровоцировал взрыв на этом предприятии, в результате которого было разрушено более 1000 центрифуг [42]. Для Ирана это ознаменовало откат в развитии ядерной отрасли на несколько лет. Для мира – начало эпохи чрезвычайно разрушительного противоборства международных акторов в киберпространстве. Грянувшая в 2020 году пандемия COVID-19 только усилила проникновение информационных технологий во все сферы деятельности, чем спровоцировала увеличение числа кибератак. Например, согласно отчету Group-IB, количество атак такого рода на российскую критическую инфраструктуру в первом полугодии 2021 года по сравнению с 2019 годом выросло более, чем в 3 раза [15]. Следовательно, вопросы обеспечения международной информационной безопасности сегодня актуальны, как никогда. Уже с 1990-х годов эта проблема является объектом пристального внимания ООН – организации, которая смогла вовлечь наибольшее число государств в её обсуждение и продолжает активно работать над выработкой универсальных мер по созданию безопасной международной информационной среды и защите от исходящих из киберпространства угроз.

https://doi.org/10.52605/16059921_2022_05_80

1 Международная информационная безопасность

В свете того, что информационные технологии активно развиваются, информационное пространство претерпевает постоянные изменения. Модифицируются и угрозы, исходящие из него. О возрастающей чреватой опасностью роли киберпространства в рамках международной информационной безопасности писал и Дж. Най. В концепции киберсилы он подчеркивал способность оказывать информационное влияние на политическую, социальную и экономическую сферы международного сообщества через интернет-пространство, использовать информацию как инструмент доминирования [40].

Динамичность и многоаспектность международной информационной безопасности определяет необходимость постоянной актуализации категориального аппарата, в частности понятия «международная информационная безопасность», выявления её базовых характеристик, а также уточнение смежных с ней понятий с целью наиболее глубокого понимания и изучения не только этой проблемы, но и всех социальных процессов современного информационного общества.

Ядром термина «международная информационная безопасность» является понятие «**безопасность**». Под безопасностью как таковой понимается либо отсутствие опасности [29], либо стабильное функционирование и состояние защищенности субъекта от опасности, возможность и готовность ей противостоять. Именно второе значение закреплено в Стратегии национальной безопасности Российской Федерации от 2016 г., где безопасность определяется как «состояние защищенности личности, общества и государства от внутренних и внешних угроз» [31].

Для того, чтобы приблизиться к определению термина «международная информационная безопасность», есть смысл обратиться к исходному понятию «**информационная безопасность**». Международной организацией по стандартизации и Международной электротехнической комиссией был разработан стандарт по информационной безопасности ISO/IEC 27001 [38], где этот термин определяется как процесс обеспечения конфиденциальности, целостности и доступности информации. Это определение интересно тем, что включает в себя триаду CIA (confidentiality с англ. – «конфиденциальность», integrity с англ. – «целостность», availability с англ. – «доступность») – ключевые принципы информационной безопасности, сформулированные американскими программистами Д. Зальцером и М. Шрёдером в 1975 году [36].

С развитием информационных технологий и их внедрения во все сферы жизни понадобилось осмыслить не только техническую, но и социальную сторону обсуждаемого термина. Так, профессор Академии военных наук С.И. Макаренко в предлагаемом им варианте определения («информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры» [20]) акцентирует, что нарушение информационной безопасности может быть преднамеренным или случайным, что оно наносит ущерб людям и организациям, имеющим к ней отношение. Нельзя не отметить, что информационная безопасность включает в себя как защиту самой информации, так и защиту от информации [4], что С.П. Расторгуевым понимается как защита от «опасной», «неадекватной картине мира информации» [27].

Не последнюю роль в определении понятия **международной информационной безопасности** играют документы межгосударственного уровня, разработанные ООН. Так, в Докладе ГА ООН от 10 июля 2000 года дается следующее определение: «это состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве». Под угрозой здесь понимается совокупность условий и факторов, создающих опасность для международной безопасности в информационном пространстве и подвергающих риску стабильность мира в целом.

В терминах ООН под международной информационной безопасностью понимается защищенность глобальной информационной системы от «триады угроз» – террористической, преступной и военно-политической. Последний вид подразумевает информационное противоборство и информационные войны. В 2013 году Россией в документе «Основы государственной политики в области международной информационной безопасности до 2020 года» [25] к триаде угроз были добавлены угроза вмешательства во внутренние дела государства посредством информационно-коммуникационных технологий, что нарушает государственный

суверенитет, а также нарушение общественной стабильности посредством разжигания вражды на основе разницы в этносах, национальностях, расах.

Более того, исследователями выделяются либеральный и реалистический подходы к понимаю международной информационной безопасности. Согласно либеральному подходу, путь к обеспечению информационной безопасности на межгосударственном уровне лежит через:

1) заключение многосторонних соглашений;
2) создание сети международных организаций;
3) усиление в и взаимозависимости государств в информационной сфере, основанных на взаимном доверии и следовании принятым соглашениям;
4) либерализацию международных отношений в сфере информации [4].

Реалистический подход фокусируется на:

1) повышении уровня национальной информационной безопасности (например, посредством создании внутренних сетей, независимых от глобальной информационной сети);
2) постоянных наблюдений и оценке информационной безопасности потенциальных противников и поиск их уязвимостей в этой сфере;
3) разработке стратегий ведения информационных войн;
4) уменьшении взаимодействия и взаимозависимости государств в информационной сфере;
5) уменьшении открытости международных отношений в сфере информации [5].

В зависимости от страны, её положения на мировой арене и её внешнеполитического курса разнится и подход к трактовке вопросов международной информационной безопасности. Например, для США характерен скорее реалистический подход, так как политика государства в этой области акцентируется прежде всего на технических аспектах безопасности, в связи с чем чаще используется термин «кибербезопасность». Позицию США особенно важно рассматривать в контексте данной проблемы, так как страна осуществляет контроль над ресурсами сети Интернет, используемыми большинством населения мира.

Россия же выступает с позиции, согласно которой в международную информационную безопасность включаются как технические аспекты (безопасность и защищенность информационных сетей и систем), так и политико-идеологические, политико-психологические аспекты (например, манипулирование информацией, пропаганда посредством глобальных информационных сетей, различные формы информационного воздействия). Учитывая, что именно инициатива России послужила отправной точкой для активизации обсуждения проблем информационной безопасности в рамках ООН (на 53-й сессии ГА ООН в 1998 г. Россией был представлен проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»), можно сказать, что страна стремится продвигать либеральных подход для обеспечения международной информационной безопасности.

Таким образом, в итоге под международной информационной безопасностью можно понимать такое состояние международных отношений, при котором исключено нарушение мировой стабильности, а глобальная информационная система защищена от террористических, преступных и военно-политических угроз, в ней нет места разжиганию межэтнической, межнациональной розни и вмешательству во внутренние дела государства посредством информационно-коммуникационных технологий. Обеспечение устойчивого развития государства, поддержание стабильности и безопасности общества – все это возможно только при обеспечении международной информационной безопасности. Важность её обеспечения – обязательный пункт современной политической повестки. Однако подходы к пониманию информационной безопасности в международных отношениях отличаются у разных стран, что усложняет процесс борьбы с угрозами, исходящими из киберпространства.

2 Деятельность ООН по обеспечению международной информационной безопасности

ООН как организация, с момента своего основания занимающаяся глобальными проблемами и вопросами планетарного масштаба, не могла обойти стороной коренные сдвиги в сфере информационно-коммуникационных технологий. Организация не только пристально следила за всевозрастающей ролью информационных технологий в различных сферах жизни общества, но и оперативно создавала новые подразделения и специальные рабочие группы для того, чтобы справляться с вызовами информационно-технологической революции.

Так, учрежденный в 1978 г. Комитет по информации ГА ООН одной из целей деятельности имеет содействие установлению широкого и сбалансированного распространения информации ради укрепления мира и международного понимания. Уже в докладе Комитета по информации 1991 г. отмечалось, что ускоренное развитие технологий в развитых странах усложняет для развивающихся стран процесс информирования внешнего мира об их ценностях и точках зрения. Уточняется, что по состоянию на 1991 г. более 80% населения мира не могли внести полноценный вклад в обеспечение «мира во всем мире, взаимопонимания и прогресса», так как не имели доступа к современным на тот момент средствам информации и коммуникации [10]. В докладе Комитета по информации 1993 г. вновь подчеркивался дисбаланс в доступе к современным технологиям связи, а также констатировалось, что мир переживает информационную революцию [11]. Доклад Комитета по информации от 1997 г. заключает, что информация является одним из наиболее важных средств содействия политическому, социальному и экономическому развитию, поэтому использовать её нужно разумно и ответственно. Важно отметить, что одна из делегаций, принимавших участие в работе Комитета, заявила об информационной агрессии в адрес представляемой страны. Агрессией признавалась трансляция другим государством теле- и радиопередач, направленных на манипулирование общественным мнением с целью нарушения и подрывания социального порядка [12].

Таким образом, был признан новый вид угроз: информационная угроза государственному суверенитету. В связи с этим поступило предложение создать международный кодекс поведения в области информационного обмена, что и было сделано только в 2011 г. ЮНЕСКО. В докладе Комитета по информации от 1999 г. отмечается уже не один пример агрессии подобного рода. Так, кроме бескровной, но все же неприятной «радиоагрессии» одного государства в адрес другого, упоминается и бомбардировка национальной вещательной организации одного из государств, что расценивается как недопустимое нарушение принципа свободы информации [13].

Из вышесказанного следует, что к концу XX в. всевозрастающая роль информации и активное распространение информационно-коммуникационных технологий стали фактором, обостряющим международные отношения. Назрела необходимость внести качественные изменения в работу ООН в области информации. Инициатором этих изменений стала делегация из России. Так, начало международному обсуждению проблем информационной безопасности на общемировом уровне было положено в 1998 году. Именно тогда, на 53-й сессии ГА ООН был принят проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [28]. Впервые на международном уровне было признано, что использование информационных технологий затрагивает интересы всего мирового сообщества. Также отмечалось, что широкое распространение информационных технологий несет потенциальные угрозы как безопасности каждого государства, так и стабильности мира в целом, потому как высокие технологии могут эксплуатироваться преступниками и террористами. С 1998 г. такие резолюции ежегодно представляются ГА ООН. Принятой в 1999 г. резолюцией ГА ООН признается, что негативное влияние информационных технологий возможно не только в гражданской, но и в военной сферах.

Первым значительным достижением в работе ООН по вопросу обеспечения информационное безопасности на межгосударственном уровне стало решение о создании Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ) на 56-й сессии ГА ООН в 2001 году. Начала работу ГПЭ из 15 правительственных экспертов, выбранных на основе справедливого географического распределения, в 2004 году. Её возглавил российский дипломат А.В. Крутских. Были проведены три сессии, в рамках которых произошел широкий обмен мнениями по заданной теме, но консенсуса добиться не удалось, так как против выступил эксперт из США [7].

Второй состав ГПЭ начал работу в 2009 г. и закончился консенсусным докладом. В нем четко обозначены источники угроз информационно-технологического характера. Таковыми являются:

1) преступные элементы;
2) террористы;
3) государства.

Среди наиболее опасных угроз выделяются активизация хакеров, разработка информационных технологий как инструментов ведения разведки и войн, повышение уязвимости критической инфраструктуры в связи с её цифровизацией. Ключевой рекомендацией является продолжение диалога в этой сфере, осуществление обмена информацией о национальных законах

и национальных стратегиях в этой области, выработка общего категориального аппарата и оказание помощи развитым странам.

Третий состав ГПЭ осуществлял деятельность в 2012-2013 гг. и тоже увенчался принятием консенсусного доклада. Три его раздела посвящены рекомендациям странам-участникам ООН. Предлагается, чтобы государства активнее сотрудничали в правовой сфере, развивали практическое сотрудничество между правоохранительными органами, создавали двусторонние, региональные и многосторонние консультативные структуры с целью обмена опытом по пресечению противоправной деятельности в области международной информационной безопасности [8].

Доклад 2015 г., опубликованный по результатам четвертого состава ГПЭ, закрепил основные направления деятельности ООН по обеспечению международной информационной безопасности:

- разработка правил ответственного поведения государств в глобальном информационном пространстве;
- разработка концепции конвенции ООН «Об обеспечении международной информационной безопасности»;
- разработка проекта универсальной конвенции о сотрудничестве в сфере противодействия информационной преступности;
- продвижение концепции конвенции по безопасным работе и развитию сети Интернет [9].

После 2015 г. процесс обсуждения вопросов международной информационной безопасности изменился. Пятый созыв Группы правительственных экспертов, состоявший уже из экспертов-представителей 25 стран, не смог принять консенсусный доклад. Ключевой проблемой стало расхождение во взглядах РФ и США по вопросу о реагировании на кибератаки. РФ в этом случае считает недопустимым применение силы без санкции Совета Безопасности ООН, в то время как США отстаивает право на самооборону и использованием в том числе и военных средств.

Результатом расхождения во мнениях стало создание в 2018 г. двух параллельных форматов: Рабочей группы открытого состава ООН и Группы правительственных экспертов ООН [26]. Россия выступила за «более демократический, инклюзивный и транспарентный» переговорный процесс, который предложила реализовать через создание Рабочей группы открытого состава. По замыслу инициаторов, в таком формате могли бы принять участие все заинтересованные государства-члены, а в формате консультаций — представители деловой и бизнес-среды, НПО, научного сообщества. США же предложили созвать очередную Группу правительственных экспертов для продолжения дискуссии в узком составе.

Предложенный Россией формат сотрудничества был поддержан большинством стран ООН, до этого не участвовавших в переговорном процессе. За два года работы на заседаниях рабочей группы открытого состава выступило более 90 государств, что составляет почти половину стран-членов ООН. К тому же треть из них не являются участниками нынешнего и не были участниками предыдущих составов группы правительственных экспертов. Главным практическим шагом, к которому пришли страны в рамках работы в таком формате, стала рекомендация назначить контактных лиц, ответственных за вопросы информационной безопасности на разных уровнях: политическом и дипломатическом, военном и техническом. Это необходимо для того, чтобы упростить и улучшить коммуникацию между странами в этой области.

Таким образом, на сегодняшний день ООН можно считать центральным органом, координирующим работу по международному противодействию различным видам информационных угроз. Обсуждение вопросов обеспечения международной информационной безопасности, идущее изначально в рамках ГПЭ, а теперь и в двух форматах – ГПЭ и РГОС, несмотря на разногласия, позволяет постепенно вырабатывать общие для государств рекомендации по противодействию исходящим из киберпространства угрозам и повышать уровень защищенности мирового сообщества в информационной среде.

Заключение

Обеспечение международной информационной безопасности – одна из главных задач современности. Возможность обеспечить защищенность в информационной сфере, готовность противостоять угрозам, исходящим из киберпространства – все это является неотъемлемой частью политики государств и международных организаций. Это включает защищенность глобальной информационной системы от террористических, преступных и военно-политических угроз,

разжигания межэтнической, межнациональной розни и нарушения стабильности мирового сообщества в информационном пространстве. Специфика международной информационной безопасности заключается в том, что она подразумевает обеспечение развития каждого отдельного государства без нанесения вреда другим государствам, их мирное существование и как самостоятельных единиц, и как структурных единиц всего мирового сообщества. Процесс выработки универсальных механизмов в этой области сложен, однако, видится, что противоречия в обсуждениях данной проблемы не символизируют неразрешимый конфликт, а указывают на долгий, но вполне реальный путь к компромиссу.

Литература

1. Атаманов Г.А. Опасности субъектов информационных отношений / Г.А. Атаманов // Защита информации. Инсайд. 2014. № 5 (59). С. 9-13.
2. Бойко С.М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. 2016. № 8. С. 53-71.
3. Бойко С. Формирование системы международной информационной безопасности: российские подходы и инициативы // Международная жизнь. 2018. № 5. С. 100-110.
4. Болгов Р.В. Деятельность ООН в области информации и международные аспекты информационной безопасности России // Сравнительная политика. 2019. №1. С. 59-70.
5. Болгов Р.В., Васильева Н.А., Виноградова С.М., Панцерев К.А. Информационное общество и международные отношения / Отв. Ред. Панцерев К.А. СПб, 2014. 384 с.
6. ГОСТ Р ИСО/МЭК 27000-2012 : Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. URL: https://docs.cntd.ru/document/1200102762 (дата обращения: 13.02.2022).
7. Доклад ГПЭ ООН 2010 г. A/65/201 от 30 июля 2010 г. URL: https://documents-dds-ny.un.org/doc/ UNDOC/GEN/N05/453/65/PDF/N0545365.pdf?OpenElement (дата обращения: 13.04.2022).
8. Доклад ГПЭ ООН 2013 г. A/68/98 от 24 июня 2013 г. URL: https:// documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement (дата обращения: 13.04.2022).
9. Доклад ГПЭ ООН 2015 г. A/70/174. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 13.04.2022).
10. Доклад Комитета по информации ООН 1991 г. A/46/21 от 14 августа 1991 г. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N91/264/20/IMG/N9126420.pdf?OpenElement (дата обращения: 13.04.2022).
11. Доклад Комитета по информации ООН 1993 г. A/48/21. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N93/386/14/PDF/N9338614.pdf?OpenElement (дата обращения: 13.04.2022).
12. Доклад Комитета по информации ООН 1997 г. A/52/21. URL: https://daccess-ods.un.org/tmp/7999107.837677.html (дата обращения: 13.04.2022).
13. Доклад Комитета по информации ООН 1999 г. A/54/21 от 3-14 мая 1999 г. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/167/93/PDF/N9916793.pdf?OpenElement (дата обращения: 13.04.2022).
14. Илюшенко В. Н. Информационная безопасность общества / Томск: Томский государственный университет систем управления и радиоэлектроники, 1998. 64 с.
15. Киберугроза номер один: количество атак шифровальщиков выросло за год более чем на 150%. URL: https://www.group-ib.ru/media/ransom/ (дата обращения: 03.04.2022).
16. Конвенция об обеспечении международной информационной безопасности (концепция). URL: https://www.mid.ru/tv/?id=1698725&lang=ru (дата обращения: 13.02.2022).
17. Крутских А. Мировое сообщество стало на шаг ближе к «вакцине» от киберпреступности // Международная жизнь. 2021. № 8. С. 28-35.

18. Крыжановская И.И. Информационная безопасность как один из важнейших компонентов национальной безопасности государства // Донецкие чтения 2016. Образование, наука и вызовы современности. 2016. С. 238-239.
19. Мазуров В.А. Понятие и принципы информационной безопасности / В.А. Мазуров, В.В. Невинский // Известия Алтайского государственного университета. 2003. No 2. С. 57-63.
20. Макаренко С.И. Информационная безопасность: учебное пособие. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. 372 с.
21. Матяш С.А. Проблемы информационной безопасности личности в современных условиях // Материалы Афанасьевских чтений. 2013. No 11. С. 154-164.
22. А.В. Крутских, А.В. Бирюков, С.М. Бойко. Международная информационная безопасность: Теория и практика. Москва : Общество с ограниченной ответственностью Издательство «Аспект Пресс», 2019. 326 с.
23. Науменко, Т.В. Методологический анализ концепции информационного общества / Т. В. Науменко // Информационное общество. 2018. № 2. С. 4-9.
24. Науменко, Т.В. Что такое информационное общество? / Т. В. Науменко // Информационное общество. 2021. № 6. С. 9-16.
25. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 14.02.2022).
26. Пелевина Е.С. Особенности системы информационной безопасности как элемента международной безопасности в современном мире // Теории и проблемы политических исследований. 2017. Том 6. No 1А. С. 194-205.
27. Расторгуев С. П. Основы информационной безопасности - М.: Издательский центр «Академия», 2009. 186 с.
28. Резолюция 53/70, принятая Генеральной Ассамблеей ООН Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». URL: https://undocs.org/ru/a/res/53/70 (дата обращения: 15.02.2022).
29. Словарь Ушакова. URL: https://ushakovdictionary.ru/word.php?wordid=2007 (дата обращения 13.12.2021).
30. Терещук В.И. Проблема управления интернетом как фактор международной и национальной информационной безопасности // Studia Humanitatis. 2015 No 2. С. 1-12.
31. Указ Президента Российской Федерации от 31 декабря 2015 года N 683 «О Стратегии национальной безопасности Российской Федерации». URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (дата обращения 13.12.2021).
32. Указ Президента РФ от 5 декабря 2016 г. No 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Доступ из из справочно-правовой системы «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения 16.02.2022).
33. Фарвазова Ю.Р. Совершенствование информационной безопасности как части антитеррористической стратегии России // Вестник Казанского юридического института МВД России. 2014. № 1 (15). С. 115-120.
34. Шакиров О. ООН считает применение кибероружия все более вероятным. URL: https://expert.ru/2021/03/23/oon-i-kiberugrozy-peregovory-zaversheny-da-zdravstvuyut-peregovory/ (дата обращения: 15.02.2022).
35. Шободоева А.В. Развитие понятия «Информационная безопасность» в научно-правовом поле России // Известия БГУ. 2017. No1. С. 73-79.
36. H. Saltzer, Michael D. Schroeder // Proceedings of the IEEE. USA : IEEE, 1975. Vol. 63, no. 09 (September). P. 1281.
37. Information Security Management Using O-ISM3. URL: https://www.ism3.com/node/42 (дата обращения: 13.02.2022).
38. ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems — Overview and vocabulary. URL: https://www.iso.org/standard/41933.html (дата обращения: 16.02.2022).
39. Les États-Unis «responsables» d'une cyber-attaque contre l'Iran. URL: https://www.lapresse.ca/international/dossiers/nucleaire-iranien/201101/17/01-4360983-les-etats-unis-responsables-dune-cyber-attaque-contre-liran.php (дата обращения: 13.04.2022).
40. Nye J. Cyber Power. Cambridge: Belfer Center for Science and International Affairs, 2010. 28 p.

41. Parker Donn B. Fighting Computer Crime : A New Framework for Protecting Information — N.Y.: John Wiley & Sons, 1998. 56 p.
42. Stuxnet: начало. URL: https://www.kaspersky.ru/blog/stuxnet-victims-zero/6119/ (дата обращения: 15.02.2022).

INTERNATIONAL INFORMATION SECURITY AS A MODERN ISSUE

Prokhorova, Daria Alexandrovna

Lomonosov Moscow State University, Faculty of global studies, master
Moscow, Russian Federation
dularno@yandex.ru

Abstract

This article examines the role of information and information technologies in the contemporary world. Not only are they a symbol of modern social development, but also a harbinger of new threats to international security. The features of the concepts of «security», «information security» and «international information security» are reviewed, as well as the role of the UN as a key international coordinator of international information security activities and the working groups and specialized organizations operating within the UN on this topic. The necessity of creation and future development of the categorical apparatus, contributing to the in-depth study of information issues and information security issues, is justified.

Keywords

international information security, UN, Committee on Information, information, security, protectability

References

1. Atamanov G.A. Opasnosti sub"yektov informatsionnykh otnosheniĭ / G.A. Atamanov // Zashchita informatsii. Insaĭd. 2014. № 5 (59). C. 9-13.
2. Boyko S.M. Gruppa pravitel'stvennykh ekspertov OON po dostizheniyam v sfere informatizatsii i telekommunikatsiy v kontekste mezhdunarodnoy bezopasnosti: vzglyad iz proshlogo v budushcheye // Mezhdunarodnaya zhizn'. 2016. № 8. S. 53-71.
3. Boyko S. Formirovaniye sistemy mezhdunarodnoy informatsionnoy bezopasnosti: rossiyskiye podkhody i initsiativy // Mezhdunarodnaya zhizn'. 2018. № 5. S. 100-110.
4. Bolgov R.V. Deyatel'nost' OON v oblasti informatsii i mezhdunarodnyye aspekty informatsionnoy bezopasnosti Rossii // Sravnitel'naya politika. 2019. №1. S. 59-70.
5. Bolgov R.V., Vasil'yeva N.A., Vinogradova S.M., Pantserev K.A. Informatsionnoye obshchestvo i mezhdunarodnyye otnosheniya / Otv. Red. Pantserev K.A. SPb, 2014. 384 s.
6. GOST R ISO/MEK 27000-2012: Informatsionnaya tekhnologiya (IT). Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti. Obshchiy obzor i terminologiya. URL: https://docs.cntd.ru/document/1200102762 (accessed on 13.02.2022).
7. Doklad GPE OON 2010 g. A/65/201 ot 30 iyulya 2010 g. URL: https://documents-dds-ny.un.org/doc/ UNDOC/GEN/N05/453/65/PDF/N0545365.pdf?OpenElement (accessed on 13.04.2022).
8. Doklad GPE OON 2013 g. A/68/98 ot 24 iyunya 2013 g. URL: https:// documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement (accessed on 13.04.2022).
9. Doklad GPE OON 2015 g. A/70/174. URL: https://documents-dds-ny.un.org/ doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (accessed on 13.04.2022).
10. Doklad Komiteta po informatsii OON 1991 g. A/46/21 ot 14 avgusta 1991 g. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N91/264/20/IMG/N9126420.pdf?OpenElement (accessed on 13.04.2022).
11. Doklad Komiteta po informatsii OON 1993 g. A/48/21. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N93/386/14/PDF/N9338614.pdf?OpenElement (accessed on 13.04.2022).
12. Doklad Komiteta po informatsii OON 1997 g. A/52/21. URL: https://daccess-ods.un.org/tmp/7999107.837677.html (accessed on 13.04.2022).
13. Doklad Komiteta po informatsii OON 1999 g. A/54/21 ot 3-14 maya 1999 g. URL: https://documents-dds-

ny.un.org/doc/UNDOC/GEN/N99/167/93/PDF/N9916793.pdf?OpenElement (accessed on 13.04.2022).
14. Ilyushenko V. N. Informatsionnaya bezopasnost' obshchestva / Tomsk: Tomskiy gosudarstvennyy universitet sistem upravleniya i radioelektroniki, 1998. 64 s.
15. Kiberugroza nomer odin: kolichestvo atak shifroval'shchikov vyroslo za god boleye chem na 150%. URL: https://www.group-ib.ru/media/ransom/ (accessed on 03.04.2022).
16. Konventsiya ob obespechenii mezhdunarodnoy informatsionnoy bezopasnosti (kontseptsiya). URL: https://www.mid.ru/tv/?id=1698725&lang=ru (accessed on 13.02.2022).
17. Krutskikh A. Mirovoye soobshchestvo stalo na shag blizhe k "vaktsine" ot kiberprestupnosti // Mezhdunarodnaya zhizn'. 2021. № 8. S. 28-35.
18. Kryzhanovskaya I.I. Informatsionnaya bezopasnost' kak odin iz vazhneyshikh komponentov natsional'noy bezopasnosti gosudarstva // Donetskiye chteniya 2016. Obrazovaniye, nauka i vyzovy sovremennosti. 2016. S. 238-239.
19. Mazurov V.A. Ponyatiye i printsipy informatsionnoy bezopasnosti / V.A. Mazurov, V.V. Nevinskiy // Izvestiya Altayskogo gosudarstvennogo universiteta. 2003. No 2. S. 57-63.
20. Makarenko S.I. Informatsionnaya bezopasnost': uchebnoye posobiye. Stavropol': SF MGGU im. M. A. Sholokhova, 2009. 372 s.
21. Matyash S.A. Problemy informatsionnoy bezopasnosti lichnosti v sovremennykh usloviyakh // Materialy Afanas'yevskikh chteniĭ. 2013. No 11. S. 154-164.
22. A.V. Krutskikh, A.V. Biryukov, S.M. Boyko. Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika. Moskva: Obshchestvo s ogranichennoy otvetstvennost'yu Izdatel'stvo "Aspekt Press", 2019. 326 s.
23. Naumenko, T.V. Metodologicheskiy analiz kontseptsii informatsionnogo obshchestva / T. V. Naumenko // Informatsionnoye obshchestvo. 2018. № 2. S. 4-9.
24. Naumenko, T.V. Chto takoye informatsionnoye obshchestvo? / T. V. Naumenko // Informatsionnoye obshchestvo. 2021. № 6. S. 9-16.
25. Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti mezhdunarodnoy informatsionnoy bezopasnosti na period do 2020 goda. URL: http://www.scrf.gov.ru/security/information/document114/ (accessed on 14.02.2022).
26. Pelevina Ye.S. Osobennosti sistemy informatsionnoy bezopasnosti kak elementa mezhdunarodnoy bezopasnosti v sovremennom mire // Teorii i problemy politicheskikh issledovaniĭ. 2017. Tom 6. No 1A. S. 194-205.
27. Rastorguyev S. P. Osnovy informatsionnoy bezopasnosti. M.: Izdatel'skiy tsentr «Akademiya», 2009. 186 s.
28. Rezolyutsiya 53/70, prinyataya General'noy Assambleyey OON Dostizheniya v sfere informatizatsii i telekommunikatsiĭ v kontekste mezhdunarodnoy bezopasnosti». URL: https://undocs.org/ru/a/res/53/70 (accessed on 15.02.2022).
29. Slovar' Ushakova. URL: https://ushakovdictionary.ru/word.php?wordid=2007 (data obrashcheniya 13.12.2021).
30. Tereshchuk V.I. Problema upravleniya internetom kak faktor mezhdunarodnoy i natsional'noy informatsionnoy bezopasnosti // Studia Humanitatis. 2015 No 2. S. 1-12.
31. Ukaz Prezidenta Rossiyskoy Federatsii ot 31 dekabrya 2015 goda N 683 "O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii". URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (data obrashcheniya 13.12.2021).
32. Ukaz Prezidenta RF ot 5 dekabrya 2016 g. No 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii". Dostup iz iz spravochno-pravovoy sistemy «Garant». URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (data obrashcheniya 16.02.2022).
33. Farvazova YU.R. Sovershenstvovaniye informatsionnoy bezopasnosti kak chasti antiterroristicheskoy strategii Rossii // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2014. № 1 (15). S. 115-120.
34. Shakirov O. OON schitayet primeneniye kiberoruzhiya vse boleye veroyatnym. URL: https://expert.ru/2021/03/23/oon-i-kiberugrozy-peregovory-zaversheny-da-zdravstvuyut-peregovory/ (accessed on 15.02.2022).
35. Shobodoyeva A.V. Razvitiye ponyatiya "Informatsionnaya bezopasnost'" v nauchno-pravovom pole Rossii // Izvestiya BGU. 2017. No1. S. 73-79.
36. H. Saltzer Saltzer, Michael D. Schroeder // Proceedings of the IEEE. USA : IEEE, 1975. Vol. 63, no. 09 (September). P. 1281.

37. Information Security Management Using O-ISM3. URL: https://www.ism3.com/node/42 (accessed on 13.02.2022).
38. ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary. URL: https://www.iso.org/standard/41933.html (accessed on 16.02.2022).
39. Les États-Unis "responsables» d'une cyber-attaque contre l'Iran. URL: https://www.lapresse.ca/international/dossiers/nucleaire-iranien/201101/17/01-4360983-les-etats-unis-responsables-dune-cyber-attaque-contre-liran.php (accessed on 13.04.2022).
40. Nye J. Cyber Power. Cambridge: Belfer Center for Science and International Affairs, 2010. 28 p.
41. Parker Donn B. Fighting Computer Crime : A New Framework for Protecting Information. N.Y.: John Wiley & Sons, 1998. 56 p.
42. Stuxnet: nachalo. URL: https://www.kaspersky.ru/blog/stuxnet- victims-zero/6119/ (accessed on 15.02.2022).