



**МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ И ВНЕШНЯЯ ПОЛИТИКА.
МЕЖДУНАРОДНОЕ И ЕВРОПЕЙСКОЕ ПРАВО**

УДК 341

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
И МЕЖДУНАРОДНОЕ ПРАВО**

ВАХИТОВА Гузель Валериевна

*кандидат филологических наук, доцент кафедры международного права и международных отношений Института права ФГБОУ ВО «Башкирский государственный университет», г. Уфа, Россия.
E-mail: v.guzel.v@mail.ru*

ШОНИН Николай Егорович

*кандидат политических наук, доцент кафедры международного права и международных отношений Института права ФГБОУ ВО «Башкирский государственный университет», г. Уфа, Россия.
E-mail: shonin_nick@mail.ru*

Изобретение и применение современных информационно-коммуникационных технологий является одновременно и угрозой международной безопасности и средством её обеспечения. Проблемы, возникающие в связи с распространением информационных технологий на сферу международных отношений, связаны с развитием нормативно-правовой базы по обеспечению информационной безопасности в России и в мире. Документы ООН указывают на опасность применения информативных технологий в военной сфере. О серьёзности этих угроз свидетельствует то, что только в России было принято четыре нормативно-правовых документа, посвященных специально проблемам информационной безопасности, на уровне ООН принято шесть соответствующих специальных резолюций. Проблемами информационной безопасности занимаются и неправительственные организации, особенно авторитетной из них является ПИР-центр (Россия), который обладает консультативным статусом при ЭКОСОС ООН.

Ключевые слова: законом диалектики, международной безопасности, правоохранительной области, международных отношений, международного права.

**INFORMATION TECHNOLOGY
AND INTERNATIONAL LAW**

VAKHITOVA Guzel Valerievna

*Candidate of Philological Sciences, Assistant Professor of the Chair of International Law and International Relations of the Institute of Law of the FSBEI HE "Bashkir State University", Ufa, Russia.
E-mail: v.guzel.v@mail.ru*

SHONIN Nikolay Egorovich

Candidate of Political Sciences, Assistant Professor of the Chair of International Law and International Relations of the Institute of Law of FSBEI HE "Bashkir State University", Ufa, Russia. E-mail: shonin_nick@mail.ru

The invention and application of modern information and communication technologies is both a threat to international security and a means of ensuring it. The paper considers the problems arising in connection with the spread of information technologies to the sphere of international relations, the development of the regulatory and legal framework for ensuring information security in Russia and in the world. The danger of using informative technologies in the military sphere is specially mentioned, as indicated by the UN documents. The severity of these threats is evidenced by the fact that only in Russia four normative and legal documents devoted specifically to the problems of information security were adopted, six corresponding special resolutions were adopted at the UN level. Information security issues are also handled by non-governmental organizations, especially the authoritative one is the PIR Center (Russia), which has consultative status with the UN ECOSOC.

Key words: law of dialectics, international security, law enforcement, international relations, international law.



Информационные технологии так быстро вошли в нашу жизнь, что ими охвачены все её стороны. Без них сбор, обработка, передача и сохранение информации по-прежнему оставались бы очень трудоемким процессом, требующим участия огромного количества работников и занимающим много времени. Но эти же достоинства информационных технологий в соответствии с законом диалектики превратились и в свою противоположность, порождая невиданные ранее проблемы, особенно в области обеспечения национальной и международной безопасности и в правоохранительной области. Распространившись на сферу международных отношений, эти проблемы требуют решения не только в чисто технологическом и техническом плане, но и в области международного права. В доинформационную эпоху, когда информация передавалась на бумажных носителях, дополненных затем фотодокументами и (микро-) фотопленками, передачами по радио и телевидению, контроль за информационными потоками со стороны государства осуществлялся весьма эффективно: печатные источники и отечественные теле-радиопередачи подвергались строгой цензуре, иностранные теле-радиопередачи глушились, а в 1950-60-ые годы даже запрещалось производить и продавать радиоприемники, способные принимать «вражеские голоса».

Иное дело современный мир. Если во второй половине XX века трезвомыслящие политики пришли к выводу о невозможности обеспечить национальную безопасность без обеспечения международной безопасности, то сейчас всеми осознано, что обеспечить международную безопасность без информационной безопасности невозможно. Примечательно, что гарантом безопасности тогда были само существование ядерного оружия, роковая опасность его применения. Что же касается современных информационно-коммуникационных технологий, то их изобретение и применение является одновременно и угрозой международной безопасности и средством её обеспечения. Важнейшими угрозами здесь являются в первую очередь использование информационно-коммуникационных технологий во враждебных целях против информационных инфраструктур других государств в политических, в военных и экономических целях. Особенно чреваты последствиями кибератака на энергетические сети, что парализует и экономику и обороноспособность. В современном мире происходит постепенная «информатизация» вооруженных сил и «интеллектуализация» традиционных вооружений. Информационное оружие становится важным элементом военного потенциала государств. Оно эффективно дополняет традиционные военные средства и в ряде случаев способно заменить их. В таких условиях Россия стала первым государством, которое на международном уровне подняло вопрос о появлении принципиально новых (информационных) угроз национальной и международной безопасности в XXI веке [5].

Вышеназванное отличие информационного оружия от ядерного привело к тому, что с начала XXI века межгосударственные конфликты все более приобретают форму информационных войн, поскольку они могут осуществляться без огромных инвестиций в военную технику и вооружения, а, самое главное, без обязательного объявления войны, тайно и трансгранично. Эта особенность информационного оружия позволяет использовать его достаточно скрытно не только против врагов, но и для контроля за союзниками. Известны скандалы с прослушкой американскими спецслужбами телефонных переговоров руководителей стран-членов НАТО, взламывания сайтов политических деятелей и т.д. Даже использование негосударственных субъектов оказывается здесь более приемлемым, ибо труднее доказать их деятельность для того или иного государства в отличие от так называемых частных военных компаний [8], типа Blackwater, где *сui bono* достаточно хорошо просматривается.

Еще больше подрывают международную стабильность и безопасность преступники-одиночки, так называемые хакеры, и преступные сообщества, получившие доступ к информационно-коммуникативным технологиям и разворачивающие свою деятельность в киберпространстве либо с целью обогащения, либо с политическими целями как международные террористы, потому что их больше и мотивы разнообразнее.

Впрочем, помимо этих опасных для мира хакеров есть и такие, которые работают на пользу мирового сообщества, раскрывая преступные планы правительств и организаций.



От них получает, например, информацию WikiLeaks. Поскольку информационно-коммуникационные технологии дают эффект для национальной экономики и обороны только тогда, когда они реализуются в сетях, то перед каждым государством постоянно стоит задача уберечь их от несанкционированного проникновения. Одной из составных частей решения этой задачи в демократических государствах является создание нормативно-правовой базы. Поскольку наша страна находится в центре информационных атак со стороны стран НАТО, то совершенно логично, что у нас был создан солидный нормативно-правовой блок: Федеральный закон Российской Федерации от 28 декабря 2010 г. N 390-ФЗ "О безопасности", Федеральный закон от 15 июля 1995 г. N 101-ФЗ "О международных договорах Российской Федерации" (в ред. от 25.12.2012), Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации. (Принят Государственной Думой 8 июля 2006 года. Одобрен Советом Федерации 14 июля 2006 года), Концепция внешней политики Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным 30 ноября 2016 г.), Военная доктрина Российской Федерации (Дата подписания: 25.12.2014.), Доктрина информационной безопасности Российской Федерации. (Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646), Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации"), постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (в ред. Постановлений Правительства РФ от 23.04.1996 N 509, от 29.03.1999 N 342, от 17.12.2004 N 808), ПОЛОЖЕНИЕ о Министерстве иностранных дел Российской Федерации (В редакции Указа Президента Российской Федерации от 19.10.2005 г. N 1218), Указ Президента РФ от 12 марта 1996 г. № 375 "О координирующей роли Министерства иностранных дел Российской Федерации в проведении единой внешнеполитической линии Российской Федерации", Указ Президента Российской Федерации от 7 мая 2012 г. № 605 "О мерах по реализации внешнеполитического курса Российской Федерации", Указ президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности российской федерации при использовании информационно- телекоммуникационных сетей международного информационного обмена", а также нормативные правовые акты Российской Федерации, регулирующие деятельность федеральных органов государственной власти в сфере внешней политики и иные нормативные правовые акты Российской Федерации в этой сфере.

Поскольку использование информационно-коммуникационных технологий в информационных войнах означает вмешательство во внутренние дела суверенных государств и подрывает режим доверия в отношениях между государствами, международное сообщество в лице ООН не могло оставить без внимания такую ситуацию. Примечательно, что опасность враждебного использования информационных технологий во вред мировому сообществу была осознана только на рубеже XX–XXI веков, что явно связано с пониманием американским руководством неэффективности экономических методов «холодной войны» против России и переходу к преимущественно информационной войне в духе рекомендаций А. Даллеса.

А ведь в последней трети XX века ситуация выглядела иначе. Подписывались договоры о запрещении распространения ядерного оружия (ДНЯО, 1968 г.), договоры, объявляющие безъядерными зонами огромные пространства (Об Антарктике 1959 г., О запрещении ядерного оружия в Латинской Америке (договор Тлателолко 1967 г.), О безъядерной зоне в южной части Тихого океана (договор Раратонга 1985 г.), договоры о вооруженных силах в Европе, о сокращении стратегических вооружений и потенциалов и др. Дело, казалось, шло к реальному углублению и расширению сотрудничества во всех областях, в том числе и информационной. Бурное развитие информационно-коммуникационных технологий в начале 1970-х годов позволило надеяться на улучшение перспектив более тесного сотрудничества государств в интересах мира и прогресса. На уровне ООН были приняты такие резолюции, как A/RES/2844(XXVI) от 19 декабря 1971 года «Свобода информации, права человека и научно-технический прогресс, ликвидация всех форм религиозной нетерпимости»,



A/RES/31/183 от 21 декабря 1976 года «Создание сети для обмена технической информацией», A/RES/32/178 от 19 декабря 1977 года «Сеть для обмена технической информацией и банк промышленно-технической информации».

Развал СССР породил у его противников надежду на такой же исход борьбы и с постсоветской Россией. Развал экономики и армии, разрушение всей системы обороны, осуществляемое администрацией Б. Ельцина, казалось, гарантировали такой исход. США решили, что форсировать далее этот процесс уже нет необходимости и переключились на другие цели. И просчитались. В итоге информационная война против России приняла уже откровенно оголтелый характер в форме неуправляемого потока информационной лжи. Дальше всех зашла в этом администрация нынешнего президента США Д. Трампа, не остановившаяся даже перед таким грубым нарушением принципов и норм международного права, как захват дипломатических представительств России на своей территории, а ведь Венская конвенция о дипломатических сношениях, от 18 апреля 1961 г. оговаривает право заграничных представительств на «получение всеми законными средствами информации о государстве пребывания». Венская конвенция о консульских сношениях, от 24 апреля 1963 г., ст.5 п. с) также дает право на «выяснение всеми законными путями условий и событий в торговой, экономической, культурной и научной жизни государства пребывания, сообщение о них правительству представляемого государства и предоставление сведений заинтересованными лицами».

Эта ожесточенная информационная война против России переродилась в войну всех против всех и породила новый аспект напряженности во всем мире. К концу 1990-х годов мировое сообщество вынуждено было признать необходимость борьбы за международную информационную безопасность. Первопроходцем здесь, так же, как и в XIX веке по общим вопросам международной безопасности, стала Россия, когда уже 17 декабря 1991 г. по инициативе Администраций связи 11 государств было создано Региональное содружество в области связи (РСС) с целью широкого сотрудничества и проведения согласованных действий этих государств в области электрической и почтовой связи. В соответствии с Соглашением о координации межгосударственных отношений в области почтовой и электрической связи, подписанным правительствами государств – участников СНГ (Бишкек, 9 декабря 1992 г.) данное содружество было одобрено как межгосударственный координирующий орган. РСС ныне официально признано наблюдателем в Международном союзе электросвязи и Всемирном почтовом союзе – специализированных учреждениях ООН по связи. Высшим органом РСС является Совет глав Администраций связи. Постоянно действующим исполнительным органом РСС является Исполнительный комитет, который находится в Москве [7].

Первым международным документом в этой области стали резолюции ООН A/RES/53/70 от 4 декабря 1998 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», A/RES/54/49 от 1 декабря 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», а также A/RES/55/63 от 4 декабря 2000 года и A/RES/56/121 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий» и другие общим числом 30 [3]. 8 декабря 2010 г. была принята еще одна резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (65/41). Во всех этих документах отмечается, что распространение и использование информационных технологий и средств затрагивают интересы всего международного сообщества и что широкое международное взаимодействие способствует обеспечению оптимальной эффективности, выражается озабоченность тем, что эти технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, и могут негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам, считается необходимым предотвратить использование информационных ресурсов или технологий в преступных или террористических целях, а государства-члены призываются и далее содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной без-



опасности, а также возможных стратегий по рассмотрению угроз, возникающих в этой сфере, исходя из необходимости сохранить свободный поток информации [3].

Но наиболее основательно, а главное реалистично рассматривается проблема и пути её решения в концепции Конвенции об обеспечении международной информационной безопасности, опубликованной 22 сентября 2011 г. на сайте МИД России, содержащей помимо традиционной преамбулы такие статьи: ст.1. Предмет и цель Конвенции, ст. 2. Термины и определения, ст. 3. Исключения в применении Конвенции, ст. 4. Основные угрозы международному миру и безопасности в информационном пространстве, ст. 5. Основные принципы обеспечения международной информационной безопасности, ст. 6. Основные меры предотвращения военных конфликтов в информационном пространстве, ст. 7. Меры, направленные на разрешение военных конфликтов в информационном пространстве.

Нашла отражение в концепции и такая актуальная проблема, как терроризм. Об этом говорится в гл. 3 «ОСНОВНЫЕ Меры противодействия использованию информационного пространства в террористических целях» и гл. 4 «Основные меры противодействия правонарушениям в информационном пространстве». Но осознание угроз ведь ничего не даст, если не будут приняты меры по их обузданию, а они не будут эффективны, если не возьмётся за их решение всем миром, на что и указывает этот российский проект конвенции в главе 5 «Международное сотрудничество в сфере международной информационной безопасности» [4].

Таким образом, резолюции и конвенции ООН показывают, что мировое сообщество не только осознало опасность враждебного использования информационно-коммуникационных технологий отдельными государствами или организациями особенно преступного характера, но и указало на необходимость и возможность создания таких информационных технологий, которые смогут противодействовать опасному для мира использованию существующих информационных технологий, как об этом, например, говорится гл. 5 выше названной конвенции: «...государства-участники должны поддерживать и стимулировать научно-технические разработки в области освоения информационного пространства, а также образовательно-просветительскую деятельность, направленную на формирование глобальной культуры кибербезопасности [4]. Обострение международной обстановки в настоящее время привело к тому, что ООН в августе 2015 года призвала не использовать информационные технологии в военных целях. С учетом такого развития в вузах России было даже создано направление подготовки 090000 "Информационная безопасность", специальность 090104 "Комплексная защита объектов информатизации" для студентов и слушателей факультета повышения квалификации, а также для дополнительной профессионально-образовательной программы "Преподаватель высшей школы". Выпускаются соответствующие учебники, например: Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации: учебное пособие.

В заключение следует отметить, что обеспечение информационной безопасности в международном масштабе связано с одной очень большой трудностью, на которую указал консультант ПИР-Центра [6] Адлан Маргоев в беседе с сэром Дэвидом Омандом, профессором Лондонского Королевского колледжа, бывшего в прошлом руководителем Центра правительственной связи, являющегося специальной службой Великобритании, ответственной за ведение радиоэлектронной разведки и обеспечение защиты информации. Трудность по его мнению заключается в том, что кибератаки в отличие от ограниченной ядерной войны, которую не удастся удержать в этом масштабе и она превратится в полномасштабную с соответствующими последствиями для воюющих государств и мира, поддаются ограничению, не ведут к эскалации и, следовательно, являются очень привлекательным средством в современной информационной войне [6]. Привлекательность кибератак повышается еще и тем, что определить источник практически невозможно, а значит, вероятность ответной атаки низка, так что в будущем вполне возможно, что противостояние США и России примет эту форму.

**Библиографические ссылки**

1. Атрибуция кибератаки является политическим решением, это не судебный процесс // Ядерный Контроль, выпуск № 4 (486), Май 2017 [Электронный ресурс] URL: <http://www.pircenter.org/articles/2099-atribuciya-kiberataki-yavlyaetsya-politicheskim-resheniem-eto-ne-sudebnyj-process>.
2. A/RES/55/63 от 4 декабря 2000 года и A/RES/56/121 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий». Резолюции Генеральной Ассамблеи [Электронный ресурс]. URL: <http://www.un.org/ru/development/ict/res.shtml>.
3. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Резолюция, принятая Генеральной Ассамблеей 8 декабря 2010 года [по докладу Первого комитета (A/65/405)] 65/41. Резолюции Генеральной Ассамблеи [Электронный ресурс]. URL: <http://www.un.org/ru/development/ict/res.shtml>.
4. Конвенции об обеспечении международной информационной безопасности [Электронный ресурс]. Официальный сайт МИД РФ URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.
5. Крутских Андрей. К политико-правовым основаниям глобальной информационной безопасности [Электронный ресурс]. URL: <http://www.intertrends.ru/thirteen/003.htm> (дата обращения: 15.06.2017).
6. ПИР-центр [Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/ПИР-Центр>.
7. Региональное содружество в области связи (РСС) [Электронный ресурс]. URL: <http://www.rcc.org.ru>.
8. Частные военные компании [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Частная_военная_компания.
9. [Электронный ресурс]. URL: <http://russian7.ru/post/7-glavnyx-chastnyx-armij-mira/>.
10. [Электронный ресурс]. URL: <http://politrussia.com/vooruzhennye-sily/chastnye-voennye-kompanii-469/>.

References

1. Atribuciya kiberataki yavlyaetsya politicheskim resheniem, ehto ne sudebnyj process (Attribution of cyberattacks is a political decision, this is not a trial), *Yadernyj Kontrol'*, vypusk No. 4 (486), Maj 2017 URL: <http://www.pircenter.org/articles/2099>
2. A/RES/55/63 ot 4 dekabrya 2000 goda i A/RES/56/121 ot 19 dekabrya 2001 g. «Bor'ba s prestupnym ispol'zovaniem informacionnyh tekhnologij» (Combating the criminal use of information technology), Rezolyucii General'noj Assamblei. URL: <http://www.un.org/ru/development/ict/res.shtml>
3. «Dostizheniya v sfere informatizacii i telekommunikacij v kontekste mezhdunarodnoj bezopasnosti». (Achievements in the field of information and telecommunications in the context of international security), Rezolyuciya, prinyataya General'noj Assambleej 8 dekabrya 2010 goda [po dokladu Pervogo komiteta (A/65/405)] 65/41, Rezolyucii General'noj Assamblei. URL: <http://www.un.org/ru/development/ict/res.shtml>
4. Konvencii ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti, (Convention on International Information Security), Oficial'nyj sajt MID RF. URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666
5. Krutskih Andrej. K politiko-pravovym osnovaniyam global'noj informacionnoj bezopasnosti (To the political and legal grounds of the global information security). URL: <http://www.intertrends.ru/thirteen/003.htm>
6. Regional'noe sodruzhestvo v oblasti svyazi (RSS) (Regional Commonwealth in the field of Communications). (RCC) URL: <http://www.rcc.org.ru>



7. Chastnye voennye kompanii (Private military companies). URL: https://ru.wikipedia.org/wiki/Chastnaya_voennaya_kompaniya URL: <http://russian7.ru/post/7-glavnyx-chastnyx-armij-mira/>
8. PIR-centr. URL: <https://ru.wikipedia.org/wiki/PIR-Centr>
9. URL: <http://politrussia.com/vooruzhennye-sily/chastnye-voennye-kompanii-469/>
11. URL: <http://russian7.ru/post/7-glavnyx-chastnyx-armij-mira/>

Дата поступления: 31.01.2018

Received: 31.01.2018

УДК 341.9

**АНАЛИЗ РАЗВИТИЯ ПРАВОВОГО
РЕГУЛИРОВАНИЯ ИНОСТРАННЫХ
ИНВЕСТИЦИЙ В РОССИИ**

ГУРГУЛИЯ Астанда Апполоновна

*аспирант кафедры гражданского права и
процесса Института права и национальной
безопасности Российской академии народно-
го хозяйства и государственной службы при
Президенте РФ, г. Москва, Россия.
E-mail: gurguliya93@mail.ru*

**THE ANALYSIS OF THE DEVELOPMENT
OF LEGAL REGULATION OF FOREIGN
INVESTMENTS IN RUSSIA**

GURGULIYA Astanda Appolonovna

*Postgraduate Student of the Chair of Civil Law
and Procedure of the Institute of Law and Na-
tional Security of the Russian Presidential
Academy of National Economy and Public Ad-
ministration. Moscow, Russia.
E-mail: gurguliya93@mail.ru*

В условиях неконтролируемого «бегства капитала» и неудачными попытками «деофшоризации» экономики страны стратегической задачей Российской Федерации является поиск оптимальных путей привлечения инвестиций и репатриирование капитала в экономику страны. Однако без надлежащего правового базиса, содержащего правовые гарантии для капитала, этого не удастся достичь. Инвестиционное законодательство Российской Федерации характеризуется бессистемностью, отсутствием единого закона, который устанавливал бы общие правила для различных видов инвестиционной деятельности. Анализ эволюционирования нормативно-правовой базы, регулирующей иностранные инвестиции в Российской Федерации, в особенности приток капитала в дореволюционный, советский и современный периоды, позволит найти ошибки прошлого в целях недопущения их в будущем, а также выбрать курс для эффективного развития инвестиционного законодательства.

Ключевые слова: инвестиции, правовое регулирование, экономика, иностранный капитал, концессионные соглашения.

In the conditions of uncontrolled “capital flight” and unsuccessful attempts of “deoffshorization” of the country’s economy, the strategic task of the Russian Federation at the present stage is to find the best ways to attract investments and repatriate capital to the economy of the country. However, without a proper legal framework containing legal guarantees for the capital, this will not be achieved. The investment legislation of the Russian Federation at the present stage is characterized by an unsystematic character, absence of a single law that would establish general rules for various types of investment activities. The analysis of the evolution of the regulatory framework governing foreign investments in the Russian Federation, in particular the influx of capital into the pre-revolutionary, Soviet and modern periods, will allow us to find past mistakes in order to prevent them in the future, and also to choose a course for the effective development of investment legislation.

Key words: investments, legal regulation, economy, foreign capital, concession agreements.