УДК 341.11.8

Н. О. МОРОЗ

МЕЖДУНАРОДНО-ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные технологии широко используются во всех сферах современной жизни. Злоупотребление такими технологиями может порождать угрозы не только правам физических и юридических лиц, но и национальной безопасности государства, международному миру и безопасности. Проблема обеспечения информационной безопасности является комплексной и может быть решена только посредством эффективного механизма международного сотрудничества. В связи этим статья посвящена институциональной и конвенционной форме межгосударственного сотрудничества в сфере поддержания международной информационной безопасности. Определяется роль мягкого права в контексте рассматриваемой темы. Анализируются актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий

N. O. MOROZ

INTERNATIONAL FRAMENWORK FOR INTERNATIONAL INFORMATION SECURITY

Information technologies are widely used in all spheres of modern life. Misuse of such technologies might threaten not only the rights of individuals or legal entities but also national security of states, international peace and security. The problem of ensuring information security is complex and can be solved only through an effective mechanism of international cooperation. In this connection the article is dedicated to the institutional and conventional forms of interstate cooperation in the field of maintaining international information security. The role of soft law in the context of the topic discussed is defined. The urgent issues of international cooperation in the fight against high-tech crime are analyzed.

МОРОЗ
Наталия Олеговна,
кандидат юридических наук,
заместитель заведующего
кафедрой международного права
Международного университета
«МИТСО»

Международная информационная безопасность является одним из ключевых элементов системы международной безопасности. Поддержание международной информационной безопасности – необходимое условие нормального развития международных отношений в сфере информационного обмена и использования киберпространства, обеспечения прав и свобод индивидов, юридических лиц, а также национальной безопасности государств в информационной сфере.

Следует отметить, что международная информационная безопасность имеет ряд особенностей:

1) субъектами, от которых могут исходить угрозы информационной безопасности, могут быть не только государства, но и организованные преступные группы и даже индивиды [8, с. 105–109];
2) объектами информационной безопасности выступают информационная инфраструктура государств в широком смысле, информация, массовое сознание населения [2, с. 207–208].

В настоящее время основными направлениями обеспечения международной информационной безопасности выступают:

– противодействие военно-политическим угрозам (деструктивное информационное воздействие, включая вопросы пропаганды, киберагрессия);
– противодействие преступности в сфере высоких технологий (далее – СВТ).

При этом международное сотрудничество в области поддержания международной информационной безопасности осуществляется в институциональной и конвенционной форме.

Следует отметить, что проблемам международной информационной безопасности уделяется достаточно пристальное внимание со стороны многих международных организаций, включая ООН, Организацию Договора о коллективной безопасности (далее – ОДКБ), НАТО, Шанхайскую организацию сотрудничества (далее – ШОС) и др. Координацию такого взаимодействия осуществляют как органы общей компетенции (Генеральная Ассамблея ООН, Североатлантический совет НАТО, Совет коллективной безопасности ОДКБ), органы специальной компетенции, для которых мандат в данной сфере является дополнительным (Межамериканский комитет против терроризма), специально созданные структурные единицы (Консультационный координационный центр ОДКБ по вопросам реагирования на компьютерные инциденты, Комитет по кибероборонe НАТО, Управление НАТО в сфере кибероборонe, Агентство по коммуникациям и информации НАТО и созданный в его рамках Центр по реагированию на киберугрозы, Агентство по сетевой и информационной безопасности Европейского союза, Европейский центр по киберпреступности, созданный в рамках Европола и т.д.).

Между тем сотрудничество в области обеспечения международной информационной безопасности в рамках конвенционной формы сопряжено с некоторыми проблемами. Так, в настоящее время отсутствуют комплексные международные договоры универсального

характера, регулирующие сотрудничество государств: а) в области обеспечения международной информационной безопасности; б) в борьбе с преступностью в СВТ.

Вместе с тем в доктрине широко признано, что киберпространство не является средой «вне закона» и на него также распространяются общепризнанные принципы международного права [11, с. 102–107; 15, с. 458–459; 16, с. 9; 8]. Некоторые вопросы обеспечения международной информационной безопасности частично урегулированы в различных международных договорах универсального характера. Так, ***во-первых***, враждебное использование информационных технологий, последствия и масштаб которого соизмеримы с реальным вооруженным нападением (киберагрессия), вполне определенно запрещается действующим международным правом (п. 4 ст. 2 Устава ООН). Обычно-правовой запрет совершения подобных актов признавался экспертами ООН, НАТО, ШОС [19; 23; 17]. Иначе говоря, в настоящее время запрет на применение силы или угрозы силой действует и в отношении информационного пространства.

Следует отметить, что военное реагирование на любые инциденты в киберпространстве или на акты, совершенные с использованием информационно-коммуникационных технологий, возможно лишь в полном соответствии с Уставом ООН и с полным пониманием определяющей роли Совета Безопасности ООН в данной сфере. В противном случае такие действия будут считаться неправомерными [1, с. 200; 9, с. 343–392; 25, с. 356; 15, с. 473–474].

Во-вторых, использование потенциала информационных технологий для подрыва социально-политической обстановки, осуществления деструктивного информационного воздействия, формирования общественного мнения путем распространения определенного рода информации также не является новой областью международных отношений, не урегулированных международным правом:

1) запрет негативного воздействия на общественно-политическое сознание населения, последствия которого составляют вмешательство во внутренние дела государства, также следует из действующих норм международного права (п. 7 ст. 2 Устава ООН). Недопустимость такой деятельности неоднократно подтверждалась в актах международных организаций и конференций, судебной практике (п. с Декларации о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций, от 24 октября 1970 г., п. 2 Декларации о недопустимости вмешательства во внутренние дела государств, об ограждении их независимости и суверенитета от 21 декабря 1965 г., подп. с п. I Декларации о недопустимости интервенции и вмешательства во внутренние дела государств от 9 декабря 1981 г., принцип VI разд. I Заключительного акта Совещания по безопасности и сотрудничеству в Европе от 1 августа 1975 г., п. 202–209 решения Международного суда ООН по делу о военной и военизированной деятельности в Никарагуа и против Никарагуа от 27 июня 1986 г. и др.);

2) недопустимость деструктивного информационного воздействия в настоящее время на универсальном уровне вытекает из положений ряда международных договоров (ст. 1, п. 4 ст. 2 Устава ООН, ст. 4 Международной конвенции о ликвидации всех форм расовой дискриминации от 21 декабря 1965 г., ст. 20 Международного пакта о гражданских и политических правах от 16 декабря 1966 г.), она также нашла отражение в значительном количестве резолюций Генеральной Ассамблеи ООН (п. 1 резолюции 110 (II) от 3 ноября 1947 г., п. 1 резолюции 2625 (XXV) от 24 октября 1970 г., абз. 4 п. 3, 8 резолюции 67/178 от 20 декабря 2012 г., п. 20 резолюции 67/154 от 20 декабря 2012 г. и др.);

3) распространение той или иной идеологии, формирование определенного общественного мнения путем использования глобальной информационно-телекоммуникационной сети не является принципиально новым видом деятельности. Такие действия в той или иной степени всегда использовались государствами в своих целях на протяжении всей истории [11, с. 138; 14, с. 217; 18, с. 4], и имеют устоявшееся наименование – пропаганда. В связи с тем что в настоящее время в науке не выработан единый подход к определению терминов «информационная война», «информационное оружие», в политологических работах некоторых ученых постсоветского пространства понятие «пропаганда» зачастую подменяется новым термином «информационная война», а средства осуществления такой пропаганды объявляются «информационным оружием», которое необходимо запретить с помощью международного договора [10, с. 121–122; 4, с. 146, 151, 175]. Полагаем, что это предложение нереализуемо. Критерии определения таких средств и методов воздействия должны быть предельно конкретными. Например, в соответствии с концепцией, разработанной Д. Деннинг, в качестве информационного оружия могут рассматриваться вредоносные программы, разработка, распространение и использование которых физическими и юридическими лицами, как правило, уголовно наказуемо: компьютерные вирусы; троянские программы; сетевые черви; инструменты, вызывающие отказ в обслуживании; программы-бэкдоры; фильтры системных лог-файлов для скрытия оставленных электронных следов и др. [13, с. 43–53].

Таким образом, с одной стороны, современным международным правом закрепляются основы обеспечения международной информационной безопасности, а с другой – поведение государств в информационно-коммуникационном пространстве в настоящее время подробно не регламентировано.

В целях совершенствования международно-правового сотрудничества в области информационной безопасности Российской Федерацией был подготовлен проект Конвенции об обеспечении международной информационной безопасности (далее – Конвенция) [5]. Данный документ призван комплексно регулировать как сотрудничество государств в противодействии военно-политическим угрозам в области информационной безопасности, преступности в СВТ, так и отдельные аспекты ответственного поведения государств в киберпространстве. Следует отметить, что указанный проект содержал ряд неточностей, наличие которых стало серьезным препятствием для разработки международного договора по вопросам информационной безопасности на его основе [7, с. 237–244].

В настоящее время вопросы международной информационной безопасности на универсальном уровне регулируются документами, нормы которых носят морально-политический характер и относятся к мягкому праву. По итогам работы трех групп правительственных экспертов для изучения потенциальных угроз в сфере информационной безопасности, созданных в соответствии с резолюциями Генеральной Ассамблеи ООН 58/32 от 8 декабря 2003 г., 63/70 от 2 декабря 2008 г., 68/243 от 27 декабря 2013 г., были представлены доклады, последний из которых, в частности, касался норм, правил и принципов ответственного поведения государств в киберпространстве, а также мер укрепления доверия в информационном пространстве, повышения потенциала государств в данной сфере и т. д.

Государствами – членами Шанхайской организации сотрудничества на 70-ю сессию Генеральной Ассамблеи ООН был представлен проект Кодекса поведения государств в киберпространстве, который в случае его утверждения будет создавать политические основы деятельности государств в данной сфере.

На наш взгляд, акты Генеральной Ассамблеи ООН являются базой, на основе которой может быть произведена универсальная кодификация международных норм, регулирующих сотрудничество государств в области обеспечения информационной безопасности. Более того, мягкое право, не создавая юридических обязанностей для государств, определяет цели и задачи в области обеспечения международной информационной безопасности, которые на данном этапе не все государства готовы принять в качестве правовой нормы. Полагаем также, что их последовательное выполнение способно впоследствии сформировать соответствующие международные обычные нормы. Кроме того, процесс разработки и принятия резолюций Генеральной Ассамблеи ООН проще и быстрее по сравнению с заключением международных договоров, за счет чего такие акты являются более гибким и своевременным инструментом регулирования новых международных отношений.

На региональном уровне сложилось несколько подходов к правовому регулированию сотрудничества в области обеспечения информационной безопасности в контексте противодействия военно-политическим угрозам. В рамках ШОС, СНГ, Африканского союза были заключены специальные договоры, посвященные рассматриваемой проблеме (Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г., Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности от 20 ноября 2013 г., Конвенция Африканского союза о кибербезопасности и защите персональных данных от 27 июня 2014 г.).

В НАТО и ОДКБ сотрудничество в области обеспечения информационной безопасности осуществляется на основании документов, принимаемых органами этих международных организаций (политика НАТО в области кибербезопасности, одобренная министрами обороны стран Альянса в 2014 г., план действий, принятый на Саммите НАТО в Уэльсе в 2014 г.; Решение Совета коллективной безопасности ОДКБ от 10 декабря 2010 г. «О Положении о сотрудничестве государств – членов ОДКБ в сфере обеспечения информационной безопасности», Решение Совета коллективной безопасности ОДКБ от 5 сентября 2008 г. «О Программе совместных действий по формированию системы информационной безопасности государств – членов ОДКБ» и др.).

Таким образом, в целом следует отметить, что вопросы противодействия военно-политическим угрозам в сфере информационной безопасности регулируются современным международным правом. Кроме того, действующие международно-правовые нормы налагают запрет на применение информационно-телекоммуникационных технологий в целях распространения определенного рода информации (например, в целях пропаганды войны, распространения расовой и религиозной вражды), а также вмешательства во внутренние дела государства.

В связи с указанным выше полагаем, что наиболее актуальным является вопрос правового регулирования международного сотрудничества в борьбе с преступностью в СВТ[1]. Это обусловлено тем, что взаимодействие государств по этому направлению практически не урегулировано на универсальном уровне, а рост числа заключаемых региональных специальных международных договоров в данной области ведет к выработке различных стандартов сотрудничества в борьбе с преступлениями в СВТ, что не способствует реализации принципа неотвратимости уголовной ответственности за совершение таких противоправных деяний.

Универсальное договорно-правовое сотрудничество в борьбе с преступностью в СВТ осуществляется на основании международных договоров, регулирующих борьбу государств с отдельными видами преступлений (Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000 г., Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и порнографии от 25 мая 2000 г.).

Специальные конвенции, направленные на координацию международной борьбы с преступностью в СВТ, заключены под эгидой региональных международных организаций (Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. и дополнительный протокол к ней от 21 января 2003 г., Арабская конвенция по борьбе с преступлениями в сфере информационных технологий от 21 декабря 2010 г., Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., Африканская конвенция о кибербезопасности и защите персональных данных от 27 июня 2014 г., Протокол о взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г.).

Регионализация международного сотрудничества в борьбе с преступлениями в СВТ создает ряд проблем практического характера в области противодействия

[1] См. подробнее: Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий : автореф. дис. … канд. юрид. наук : 12.00.10 / Н. О. Мороз; Белорус. гос. ун-т. – Минск, 2014. – 23 с.

таким противоправным деяниям. Например, в международных договорах, заключенных государствами на постсоветском пространстве, отсутствуют положения, регулирующие возможность получения трансграничного доступа к компьютерной информации, неотложного обеспечения сохранности хранящихся компьютерных данных сбора данных о трафике в режиме реального времени, перехвата данных о содержании и т. д.

Препятствия по сотрудничеству органов государств, принадлежащих к различным регионам, также связаны с недостаточной гармонизацией норм уголовного права в рассматриваемой сфере.

Вопрос противодействия международному кибертерроризму вызывает особое опасение у мирового сообщества. В международных договорах, заключенных на региональном уровне, нашли отражение отдельные аспекты сотрудничества государств в целях борьбы с такими противоправными деяниями. Так, кибертерроризм запрещен Арабской конвенцией по борьбе с преступлениями в сфере информационных технологий от 21 декабря 2010 г. При этом в данном международном договоре закреплен инструментальный подход к содержанию кибертерроризма, не учитывающий возможность использования информационно-коммуникационных технологий против критически важной инфраструктуры государства.

В рамках ОДКБ был заключен Протокол о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 г., который впервые закрепил специальные нормы, регулирующие вопросы сотрудничества в борьбе с деяниями, посягающими как на основы конституционного строя и безопасности государств-участников, так и на международный мир и безопасность, которые совершаются при помощи информационных технологий (ст. 3). Фактически международное сотрудничество в борьбе с кибертерроризмом входит в сферу регулирования данного международного договора.

В то же время данный документ не содержит специальных норм, регулирующих оперативное сотрудничество компетентных органов государств в целях противодействия преступлениям в информационной сфере. Так, в соответствии со ст. 6 рассматриваемого документа сотрудничество в рамках Протокола осуществляется на основании письменного обращения уполномоченного компетентного органа. Обращение, переданное с помощью технических средств связи, требует подтверждения в письменной форме. При этом такой экстраординарный способ передачи обращения возможен лишь «при получении оперативной информации о *готовящихся* (курсив мой. – *Примеч. авт.*) преступлениях», перечисленных в ст. 3 Протокола. Таким образом, из данной нормы следует, что срочный порядок сношений компетентных органов не может быть задействован по отношению к оконченным преступлениям. Между тем расследование транснациональных преступлений в СВТ требует немедленной реакции, поскольку компьютерные данные могут быть быстро удалены.

Все рассматриваемые проблемы договорно-правового регулирования сотрудничества государств в борьбе с преступностью в СВТ требуют урегулирования в международном договоре универсального характера. Следует отметить, что вопросы заключения универсального международного соглашения по борьбе с преступным использованием высоких технологий широко обсуждаются как в науке, так и на уровне ООН [2]. Сторонниками заключения универсального международного договора являются С. Шольберг [21, с. 1], Н. И. Костенко [6, с. 91–103], А. Д. Софаер, С. Е. Гудмэн [22, с. 2, 31], Р. Бродхарст [12, с. 430].

Еще на 11-м Конгрессе ООН по предупреждению преступности и уголовному правосудию говорилось о необходимости разработки универсальной международной конвенции по вопросам борьбы с преступностью в СВТ. Вместе с тем в 2015 г. на прошедшем в г. Дохе (Катар) 13-м Конгрессе ООН по предупреждению преступности и уголовному правосудию консенсус по этому вопросу так и не был достигнут.

Несомненно, в качестве «модели» для разработки национального законодательства в данной сфере может служить Инструментарий для законодательства о киберпреступности, разработанный Международным союзом электросвязи. Ряд рекомендаций по совершенствованию законодательства в данной сфере содержится в актах Генеральной Ассамблеи ООН (резолюции Генеральной Ассамблеи ООН 55/63 от 4 декабря 2000 г, 56/121 от 19 декабря 2001 г., направленные на борьбу с преступным использованием информационных технологий), ЭКОСОС ООН (преступления связанные с личными данными (резолюции ЭКОСОС 2004/26 от 21 июля 2004 г., 2007/20 от 26 июля 2007 г., 2011/35 от 28 июля 2011 г., 2009/22 от 30 июля 2009 г.)); продажа психотропных лекарств через Интернет (резолюция ЭКОСОС 2004/42 от 21 июля 2004 г.), злоупотребление новыми информационными технологиями в отношении детей (резолюция ЭКОСОС 2011/33 от 26 июля 2007 г.).

Вместе с тем таких мер в настоящее время недостаточно, поскольку модельное законодательство и рекомендации, содержащиеся в резолюциях органов международных организаций, не создают юридических обязательств для государств, а значит, не могут урегулировать отношения, связанные как с гармонизацией уголовного законодательства, так и с созданием действенной системы международного взаимодействия органов, ведущих уголовный процесс. Это обусловливает необходимость заключения международного договора о сотрудничестве государств в борьбе с преступлениями в СВТ в рамках ООН.

Таким образом, на основании изложенного выше полагаем следующее.

1. Отсутствие комплексного международного договора универсального характера, регулирующего сотрудничество государств в сфере обеспечения международной информационной безопасности, не свидетельствует об отсутствии международно-правового регулирования в исследуемой области в целом. Основы международно-правового регулирования международной информационной безопасности содержатся в действующих международных договорах универсального характера.

2. Вопросы ответственного поведения государств в киберпространстве в настоящее время целесообразно урегулировать с помощью норм мягкого права (в частности, резолюций Генеральной Ассамблеи ООН). Указанные нормы создают ориентиры для поведения государств в информационном пространстве, способствуют формиро-

ванию норм международного обычного права в рассматриваемой области.

3. Международно-правовое регулирование сотрудничества государств в борьбе с преступностью в сфере высоких технологий на универсальном уровне в настоящее время не является достаточным. Практические проблемы взаимодействия компетентных органов в целях пресечения, раскрытия и расследования таких преступлений могут быть решены исключительно посредством заключения международного договора, который должен заложить основы сотрудничества в области оказания международно-правовой помощи по таким уголовным делам, осуществления экстрадиции, а также гармонизации уголовного законодательства государств.

Список использованных источников

1. Довгань, Е. Ф. Международно-правовые основы деятельности региональных организаций в области поддержания международного мира и безопасности / Е. Ф. Довгань. – Минск: БГУ, 2014. – 295 с.
2. Довгань, Е. Ф. ОДКБ и информационная безопасность / Е. Ф. Довгань, Н. О. Мороз // Организация Договора о коллективной безопасности и планирование на случай чрезвычайных обстоятельств после 2014 г. / Н. О. Мороз [и др.] ; под ред. Е. Ф. Довгань и А. В. Русаковича; Женевский центр демократического контроля над вооруженными силами, Центр изучения внешней политики и безопасности. – Женева – Минск, 2015. – С. 207–236.
3. Доклад Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, Бангкок, 18–25 апреля 2005 г. [Электронный ресурс] // Организация Объединенных Наций. – Режим доступа : http://www.un.org/russian/events/11thcongress/a_conf203_18.pdf. – Дата доступа: 12.04.2015.
4. Информационные вызовы национальной и международной безопасности / И. Ю. Алексеева [и др.]. – М. : ПИР-Центр полит. исслед., 2001. – 328 с.
5. Конвенция об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] // Совет безопасности Российской Федерации. – Режим доступа : http://www.scrf.gov.ru/documents/6/112.html. – Дата доступа : 23.09.2012.
6. Костенко, Н. И. Правовые механизмы международного сотрудничества в правоохранительной сфере / Н.И. Костенко // Право и политика. – 2005. – № 8. – С. 91–103.
7. Мороз, Н. О. Универсальное международно-правовое регулирование сотрудничества государств в борьбе с преступностью в сфере высоких технологий / Н. О. Мороз // Правоведение. – 2014. – № 5 (316). – С. 237–244.
8. Павловский, А. А. Некоторые аспекты угроз информационной безопасности в международной сфере / А. А. Павловский // Информационная безопасность как составляющая национальной безопасности государства: материалы Междунар. науч.-практ. конф., Минск, 11–13 июля 2013 г. : в 3 т. / Ин-т нац. безопасности Респ. Беларусь; редкол. С. Н. Князев (гл. ред.) [и др.]. – Минск, 2013. – Т. 2. – С. 105–109.
9. Устав Организации Объединенных Наций от 26 июня 1945 г. // Антология мировой политической мысли : в 5 т. / ред.-науч. совет: Г. Ю. Семигин (пред.) [и др.]. – М. : Мысль, 1997. – Т. 5 : Политические документы / ред.-сост.: Ю. В. Ирхин [и др.]. – С. 343–392.
10. Юсупов, Р. М. Наука и национальная безопасность / Р. М. Юсупов. – 2-е изд., перераб. и доп. – СПб. : Наука, 2011. – С. 121–122;
11. Beard, J.M. Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law / Jack M. Beard // Vanderbilt Journal of Transn. Law. – 2014. – Vol. 47, № 1. –P. 67– 144.
12. Broadhurst, R. Developments in the global law enforcement of cyber-crime / R. Broadhurst // An Int. Journal of Police Strat. a. Management. – 2006. – Vol. 29, № 3. – P. 408–433.
13. Denning, D. Reflections on Cyberweapons Controls / D. Denning // Computer Security Journal. – 2000. – Vol. XVI, № 4. – P. 43–53.
14. Hutchinson, W. Information Warfare and Deception / W. Hutchinson // Informing Science. – 2006. – Vol. 9 – P. 217.
15. Kondoch, B. Jus ad Bellum and Cyber Warfare in Northeast Asia / Kondoch B. // Journal of East Asia and Int. Law. – 2013. – Vol. 6. – P. 473–474.
16. Lawrence, T. Greenberg. Information warfare and international law / T. Lawrence, S.E. Goodman, K.J. Soo Hoo. – Washington : Nat. Defense Univ. Press, 1998. – 53 c.
17. Letter dated 9 Jan. 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General [Electronic resource] // NATO Cooperative Cyber Defense Centre of Excellence. – Mode of access: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf. – Date of access: 23.12.2015.
18. Macdonald, S. Propaganda and Information Warfare in the Twenty-first Century: Altered Images and Deception Operations / S. Macdonald. – Abington : Routledge, 2006. – 224 p.
19. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [Electronic resource] : Seventieth session Item 93 of the General Assembly provisional agenda // The United Nations. – Mode of access: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. – Date of access: 23.12.2015.
20. Roscini, M. World Wide Warfare – Jus ad bellum and the Use of Cyber Force / Roscini M. // Max Planck Yearbook of United Nations Law. – 2010. – Vol. 14. – P. 85–130.
21. Schjolberg, S. The history of global harmonization on cybercrime legislation: the road to Geneva / S. Schjolberg // Journal of Int. Com. Law and Technology. – 2008. – Vol. 1, № 12. – P. 1–23.
22. Sofaer, A.D. Transnational dimension of cybercrime and terrorism / S.E. Goodman. – Stanford: Hoover Institution Press, 2001. – 292 p.
23. Tallinn Manual on the international law applicable to cyber warfare // Nuclearenergy.ir // [Electronic Resource]. – Mode of access : http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf. – Date of access : 20.09.2015.
24. Waxman, M.C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4) / M.C. Waxman // The Yale Journal of Int. Law – 2011. – Vol. 36. – P. 421–459.
25. Weissbrodt, D. Cyber-Conflict, Cyber-Crime, and Cyber-Espionage / D. Weissbrodt // Minnesota Journal of Int. Law. – 2013. – Vol. 22 – P. 347–387.

25.01.2016