http://www.parliament.am/legislation.php?sel=show&ID=1272&lang=rus. – Дата доступа: 04.02.2022.

11. О конкуренции : Закон Кыргызской Респ., 22 июля 2011 г. № 116 // База данных «Законодательство стран СНГ» [Электронный ресурс]. – Режим доступа: https://base.spinform.ru/show_doc.fwx?rgn=45842. – Дата доступа: 04.02.2022.

12. Договор о Евразийском экономическом союзе, подписан в г. Астане 29 мая 2014 г. // Нац. реестр правовых актов Респ. Беларусь. – 2014. – № 3/3050.

МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Старожилова Н.П., Карагандинский университет имени Е.А. Букетова

Становление современного понимания проблем информационной безопасности связано с техническим прогрессом XIX-XX вв., когда началось использование электричества, телеграфа, радио, телеграфа, телефона, радио, телевидения. Развитие технических средств связи и передачи и обработки информации стало еще более доступным после изобретения ЭВМ. Технологии сбора, обработки информации привели к осознанию и использованию ее как особого объекта, имеющего социальное, экономическое, политическое значение и восприятию информации как продукта, имеющего спрос на мировом рынке. В середине XX в. возникла проблема конкурентной борьбы за владение и способы передачи информации, на первый план вышла необходимость защиты и охраны информации, предотвращение несанкционированного ее использования. Постепенное осознание самой информации как объекта обработки и потребления способствовало постановке вопроса о праве на информацию, введении права на информацию в состав прав человека и гражданина в международных правовых актах и в национальном законодательстве государств.

В течение длительного периода инфокоммуникационные технологии (ИКТ) и информация как ресурс обработки и спроса были объектом охраны и защиты техническими (физическими) средствами, что было закреплено в законодательных актах. На их основе формировалось право на информацию, а в Республике Казахстан, России и ряде других государств это стало предметом информационного права. Аналогом является законодательство о свободе информации англоязычных и других государств.

Понимание важного значения осознания больших изменений в области использования информации как знаний и источника развития во многих направлениях жизни общества, огромное влияние и зависимость общества от уровня овладения информационными, теле-, радио-, аудио-, спутниковыми и прочими технологиями внедрило в наш обиход такие понятия, как «информационное общество», «электронное государство», «электронное правительство» (управление), «электронный гражданин», «электронное или компьютерное пространство», Интернет, киберпреступность т.д. Появление этих терминов свидетельствует о развитии глобального процесса оснащения планеты новыми технологиями и методами работы с информационными ресурсами. Это явление получило название - процесс информатизации общества и формирования нового этапа цивилизации, который именуется как «цифровая эпоха». По мнению Бачило И.Л.информационное общество является первым этапом цифровой эпохи в смене цивилизационных характеристик современного мира [1с.68].

В Концепции правовой политики Республики Казахстан в Разделе IV обозначены 13 основных направлений развития национального права. Среди них под номером 13 стоит - совершенствование регуляторной политики в сфере цифровизации и информатизации [2]. В этих условиях общество приобретает новые глобальные характеристики и качества, становясь информационным обществом. Правовая наука информационного права

определяет информационное общество как «общество создающее и использующее такой уровень инфокоммуникационных технологий, которые становятся самостоятельным социально-технологическим ресурсом жизнедеятельности и развития социума, существенно влияют на парадигмы смены его цивилизационной характеристики». Такое состояние современного общества нашло отражение в таких международных документах, как Окинавская хартия глобального информационного общества[3], Орхудская конвенция о доступе к информации [4] и др. Проблемы доступа к публичной информации обсуждаются во всем мире.

Проблемы доступа к информации влекут за собой постановку вопроса о расширении понятия гражданского общества при ориентации на главную роль человека в системеотношений организаций, граждан и органов государственной власти. Такие тенденции сегодня отмечаются в целом ряде зарубежных государств. Так, Франция живет в условиях ориентации на «цифровую администрацию», в Германии вопрос об Интернете занимает первую строку в повестке дня во внутренней политике. В августе 2014 г. федеральный Кабинет министров Германии принял «Цифровую повестку дня 2014-2017». В России в 2008 г. также принята и действует Стратегия развития информационного общества до 2020 г.[5].

В Великобритании, например, проблемам правового обеспечения безопасности персональных данных стали уделять внимание еще в восьмидесятых годах прошлого века. В этой стране правовое регулирование неприкосновенности частной жизни и персональных данных осуществляется на национальном и универсальном уровнях. Великобритания ратифицировала Конвенцию «О защите частных лиц в отношении автоматизированной обработки персональных данных» 1981 года [6]. Эта страна также выполняет требования Директивы ОЭСР «О защите неприкосновенности частной жизни и международных обменов персональными данными» от 23 сентября 1980 года [7]. К основным правовым актам национального характера относятся Закон о защите данных 1998 года [8], Закон о свободе информации 2000 года [9]. Под «данными» в Законе о защите данных понимается информация, которая обрабатывается и записывается с помощью автоматизированного оборудования и является частью системы или записью, находящегося в распоряжении государственного органа. Стоит отметить один недостаток этой формулировки. Данные могут находиться не только в распоряжении и пользовании государственного органа [10 с.72]. Очень часто такими данными обладают частные лица и организации, которые предоставляют какие-либо услуги, например, коммунальные, услуги связи. Этот же закон, например, делает различия между понятиями «конфиденциальные персональные данные» и «персональные данные». К конфиденциальным персональным данным относится информация о расовом иди этническом происхождении субъекта данных, о политических взглядах, о религиозных убеждениях, о членстве в профсоюзах, о физическом или психическом здоровье человека, о совершенных правонарушениях. Основным субъектом обеспечения конфиденциальности персональных данных является контролер данных – лицо, которое определяет цели и средства обработки персональных данных. Персональные данные могут обрабатываться и использоваться только в законных целях, которые определил контролер.

В странах англо-американской правовой системы используется понятие «кибербезопасность» [11 с.70]. В странах СНГ и в Казахстане сложился термин «информационная безопасность». Если первая рассматривает только исключительно технические угрозы Сети, например, вирусы, то в понятие информационной безопасности включается потенциально более полное содержание видов угроз, например, направленных на политическую дестабилизацию общества. Таким образом, термин «информационная безопасность» включает в себя два аспекта – информационно-технический и информационно-психологический. Этот подход нашел отражение в российской Доктрине и казахстанской Концепции информационной безопасности [12 с.11]. В Концепции

информационной безопасности Республики Казахстан сформулировано определение: «Информационная безопасность страны рассматривается в двух взаимосвязанных аспектах: техническом и социально-политическом. Технический аспект подразумевает обеспечение защиты национальных информационных ресурсов, информационных систем, информационно- телекоммуникационной инфраструктуры от неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации. Социально-политический аспект заключается в защите национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан».

Согласно классическому определению, которое дается в международном стандарте ISO/IEC 27001 и которое применяется в специализированной научной литературе, информационная безопасность включает в себя три части:

- конфиденциальность – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи);

- целостность – обеспечение точности и полноты информации, а также методов ее обработки;

- доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию).

Эти три пункта применимы только к защите данных, в то время как на так называемый социально-политический аспект они распространяться не могут. Под социально-политической составляющей информационной безопасности обычно понимают совокупность идей, а не массив данных. Даже если согласиться с тем, что защита данных и защита идей [13 с.10].могут соприкасаться друг с другом, однако это не дает достаточного основания для того, чтобы рассматривать их как два объекта информационной безопасности. Так, использование украденных государственных секретов – это проблема как защиты данных, так и защиты политической стабильности. Эти два объекта связаны между собой коммуникационными технологиями, которые становятся жизненной средой как данных, так и идей [13 с.11].

Доктрина информационного общества как гражданского, социального, демократического, правового общества сформировала проблему правового обеспечения информационной безопасности личности, государства и его системы власти, состояния общества в целом. Проблема правового регулирования содержания, распространения и использования информационных технологий на протяжении всего развития информационного общества является очень важной. Понятие «информационная безопасность» раскрыто в Докладе Генерального секретаря ООН A/55/140 от 10 июля 2010 г. Под «информационной безопасностью» понимается состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и, собственно, информацию в отношении таких ее свойств как целостность, объективность, доступность и конфиденциальность.

Глобальная информационная среда оказывает значительное влияние на состояние политической, экономической, социо-культурной и других составляющих национальной безопасности и системы международной безопасности. Развитие СМИ способствует более полной реализации человеком прав и свобод, открывает новые возможности. Обеспечение информационной безопасности необходимо для устойчивого развития мировой цивилизации, поддержания международного мира и безопасности, международного прогресса и сотрудничества. Но в то же время, существует угроза использования компьютерных сетей для совершения преступлений и правонарушений в информационном пространстве, использования информационно-коммуникационных технологий в целях нанесения ущерба безопасности как отдельного человека, так и

общества, государства, мирового сообщества. Возможно использование ИКТ в террористических, военно-политических, преступных целях, что ведет к негативным последствиям глобального масштаба. В современном мире происходит «информатизация» вооруженных сил. Появляются такие понятия, как «информационное оружие», «информационная война». Возрастает необходимость защиты от правонарушений в информационном пространстве, борьбы против распространения недостоверных или искаженных сообщений, наносящих ущерб международному миру и безопасности.

Копылов В.А. выделяет три основных направления правового обеспечения информационной безопасности:

1. защита чести, достоинства, деловой репутации от угроз воздействия вредной, опасной, недоброкачественной, недостоверной информации, нарушение порядка распространения информации;

2. защита информации и информационных ресурсов ограниченного доступа от угроз несанкционированного и неправомерного воздействия посторонних лиц;

3. защита информационных прав и свобод личности на передачу и использование информации в условиях информатизации [14 с.240]

Борьба с преступным использованием информационных технологий занимает важное место в работе международных и региональных организаций. В частности, Генеральной Ассамблеей ООН разработан ряд резолюций, регулирующих обеспечение информационной безопасности. Это Резолюция A/RES/65/141 от 20 декабря 2010 года «Использование информационно-коммуникационных технологий в целях развития», Резолюция A/RES/64/211 от 21 декабря 2009 года «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», Резолюция A/RES/64/187 от 21 декабря 2009 года «Использование информационно-коммуникационных технологий в целях развития», Резолюция A/RES/64/25 от 2 декабря 2009 года «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», резолюция A/RES/56/121 от 19 декабря 2001 года «Борьба с преступным использованием информационных технологий» и другие [15 с.27]. Обсуждением данного вопроса занимались такие региональные организации, как Шанхайская организация сотрудничества, Европейский Союз, Организация Азиатско-Тихоокеанского сотрудничества, Организация американских государств, Ассоциация стран Юго-Восточной Азии, Организация экономического сотрудничества и развития, «Группа восьми» и другие международные организации и форумы.

Данный вопрос обсуждался на встрече лидеров стран «группы восьми» в июле 2000 г. на Окинаве (Япония) при подготовке «Хартии глобального информационного общества», на Всемирной встрече на высшем уровне по вопросам информационного общества. Первый этап этой встречи проходил в декабре 2003 г. в Женеве, второй – в ноябре 2005 г. в Тунисе, на 16-й Полномочной конференции Международного союза электросвязи в Марракеше (Марокко, сентябрь-октябрь 2002 г.), на заседании совета ШОС 15 июня 2006 года. В октябре 2006 г. состоялось учредительное заседание Группы экспертов государств-членов ШОС по международной информационной безопасности.

В начале июня 2012 года в Санкт-Петербурге состоялась Третья международная встреча представителей, курирующих вопросы безопасности в государствах. Одним из основных пунктов должно было стать обсуждение предложенного российской стороной проекта **Конвенции ООН «Об обеспечении международной информационной безопасности».** Концепция конвенции об обеспечении международной информационной безопасности была представлена 22 сентября 2011 года. Проект документа разрабатывали Совет безопасности Российской Федерации, МИД Российской федерации и Институт проблем информационной безопасности МГУ. Целью Конвенции является противодействие использованию информационно-коммуникационных технологий для

нарушения международного мира и безопасности, и «установление мер предотвращения и разрешения конфликтов в информационном пространстве с учетом военных, террористических и криминальных угроз».

Под «информационной безопасностью» в Конвенции понимается состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве. Под «международной информационной безопасностью» понимается состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве [16].

Нарушениями информационной безопасности, согласно положениям Конвенции «Об обеспечении международной информационной безопасности», являются: неправомерное использование информационных ресурсов, несанкционированное вмешательство в информационные ресурсы, терроризм в информационном пространстве, использование информационных технологий и средств для осуществления враждебных действий и актов агрессии, целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства, неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы, действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество, использование международного информационного пространства государственными и негосударственными структурами, организациями, группами и отдельными лицами в террористических, экстремистских и иных преступных целях, трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств, использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду, расистских и ксенофобских письменных материалов, изображений или любого другого представления идей или теорий, которые пропагандируют, способствуют или подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии, манипулирование информационными потоками в информационном пространстве других государств, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозия традиционных культурных, нравственных, этических и эстетических ценностей, использование информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационном пространстве, противодействие доступу к новейшим информационно-коммуникационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам, информационная экспансия, приобретения контроля над национальными информационными ресурсами другого государства.

Конвенция устанавливает меры предотвращения и разрешения военных конфликтов в информационном пространстве, меры противодействия использованию информационного пространства в террористических целях, меры противодействия правонарушениям в информационном пространстве, которые включает также меры по организации уголовного процесса. В конвенции отмечено, что право каждого искать, получать и распространять информацию и идеи, как это зафиксировано в документах ООН, может быть ограничено законодательством для защиты национальной и общественной безопасности государства, а также для предотвращения неправомерного использования и несанкционированного вмешательства в информационные ресурсы.

Еще одним документом, направленным на обеспечение информационной безопасности, является Конвенция о международном праве опровержения, принятая резолюцией Генеральной Ассамблеи ООН 16 декабря 1952 года. Данная конвенция направлена на обеспечение права на полное и объективное осведомление, свободного обмена информацией и мнениями, нераспространение ложных или искаженных сведений, могущих причинить вред дружественным взаимоотношениям между государствами, повышение чувства ответственности тех, кто регулярно занимается распространением информации.

В пункте первом статьи 2 Конвенции отмечается, что «профессиональная ответственность корреспондентов и информационных агентств требует от них, чтобы они сообщали факты без дискриминации и в их надлежащей связи, поднимая тем самым уважение к правам человека и основным свободам, способствуя международному взаимопониманию и сотрудничеству и содействуя поддержанию международного мира и безопасности». В соответствии с профессиональной этикой все корреспонденты и информационные агентства должны обеспечить передачу в том же порядке или опубликование опровержений тех информационных сообщений, которые оказались ложными или искаженными.

В случае, когда государство утверждает, что информационные сообщения являются ложными и искаженными и могут нанести вред его отношениям с другими государствами и национальному престижу и достоинству, оно имеет право представить свою версию фактов («коммюнике»). Копия этого коммюнике отправляется одновременно соответствующему корреспонденту или информационному агентству, для исправления соответствующего информационного сообщения. В течение пяти суток государство, получившее коммюнике, должно передать это коммюнике работающим на его территории корреспондентам и информационным агентствам для публикации опровержения. В случае невыполнения просьбы опубликовать коммюнике, государство, предоставившее его, может обратиться с жалобой Генеральному Секретарю ООН, который оглашает это коммюнике не позднее 10 суток.

На региональном уровне Протокол о взаимодействии государств - членов Организации Договора околлективной безопасности по противодействиюпреступнойдеятельности в информационной сфере 2014 года подписан в целях выполнения обязательств о совместных действиях, направленных на формирование системы информационной безопасности государств - членов ОДКБ, реализации договоренностей по воспрепятствованию использования информационных технологий для дестабилизации обстановки на территориях государств [17].В Преамбуле отмечена необходимость защиты информационного пространства иинформационных ресурсов, оказания взаимной помощи в области предотвращения деструктивных информационных воздействий и чрезвычайных ситуаций в информационной сфере, координации оперативного реагирования на них и ликвидацию их последствий, обеспечения эффективного коллективного взаимодействия по противодействию преступной деятельности в информационной сфере и созданию правовых основ сотрудничества специальных служб и правоохранительных органов государств ОДКБ в борьбе с преступлениями в сфере информационных технологий.

В соответствии со статьей 5 сотрудничество осуществляется в следующих формах:

- Обмен информацией о готовящихся или совершенных преступлениях в сфере информационных технологий; причастных к преступлениям физических и юридических лицах; формах и методах предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере информационных технологий; новых формах и способах совершения преступлений в сфере информационных технологий; национальных законодательных и нормативных правовых актах, принятых в целях регулирования вопросов предупреждения, выявления, пресечения, раскрытия и расследования преступлений в сфере информационных технологий;

- Исполнение обращений о проведении оперативно-розыскных мероприятий, а также процессуальных действий в соответствии с международными договорами о правовой помощи и другими соответствующими международными договорами, участниками которых являются государства;

- Планирование и проведение скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере информационных технологий;

- Оказание содействия в подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров, учебных курсов и тренингов;

- Создание информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию преступлений в сфере информационных технологий.

В рамках таких международных организаций, как ШОС, ОДКБ, СНГ в разное время были также заключены многосторонние международные соглашения в области обеспечения международной информационной безопасности (Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.), Положение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в сфере обеспечения информационной безопасности (Москва, 10 декабря 2010 г.) [18].

Важным итогом реализации государственной политики в области международной информационной безопасности стало представление на 69-й сессии Генеральной Ассамблеи ООН от имени государств - членов ШОС в качестве официального документа ООН обновленной редакции Правил поведения в области обеспечения международной информационной безопасности - документа, являющегося серьезным шагом на пути формирования культуры информационной безопасности, новая редакция которого отличается от концепций, предполагающих регулирование кибервойн, миротворческим характером, нацеленным на предотвращение конфликтов в информационном пространстве.

Исследование показало, что в мировом сообществе наблюдается недостаточная активность по совершенствованию международно-договорного обеспечения информационной безопасности. Необходима разработка и принятие универсальной конвенции о глобальной информационной безопасности. Кроме этого, Республика Казахстан имеет очень низкий показатель международно-договорного обеспечения информационной безопасности. Следует активизировать работу по подготовке и заключению международных договоров о региональной информационной безопасности.

Среди угроз информационной безопасности называется такая угроза, как использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран. Источником этой угрозы является тот факт, что не все государства сегодня находятся на одинаковом уровне развития информационно-коммуникационных технологий, сохраняется также тенденция к усилению различий в таком развитии. Страны с развитыми цифровыми технологиями не должны стремиться к сохранению такого отрыва и, более того, использовать такие различия в свою пользу. Здесь в качестве аналогии можно привести ситуацию с экономическим потенциалом развивающихся стран, в отношении которых в международных экономических отношениях применяется преференциальный режим. Поэтому полагаем, что в отношении сотрудничества в информационной сфере и в целях противодействия угрозам информационной безопасности следует распространить принцип предоставления преференций и на сферу сотрудничества в информационно-коммуникационной сфере.

Список литературы:

1 Бачило И.Л., Полякова Т.А. На пути обеспечения информационной безопасности // Государство и право. – 2016. - №3. – С.66-78

2 Концепция правовой политики Республики Казахстан до 2030 года. Утв. Указом Президента Республики Казахстан от 15 октября 2021 года № 674. – [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/U2100000674

3 Окинавская Хартия глобального информационного общества (Принята 22 июля 2000 года лидерами стран G8, Окинава) – Электронный ресурс – [Режим доступа] - https://online.zakon.kz/document/

4 Конвенция о доступе к информации, участию общественности в процессе принятия решений и доступе к правосудию по вопросам, касающимся окружающей среды (Орхус, 25 июня 1998 года).) – Электронный ресурс – [Режим доступа] - https://online.zakon.kz/document/

5 Evdokimov K.N. Comparative legal analysis of the legislation of Russia and foreign countries, regulating the criminals liability for committing computer crimes // Наукаиобщество.-2016 .-№3-1 .-С.104-121

6 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981.) – Электронныйресурс – [Режимдоступа] - https://rm.coe.int/1680078b37

7 Основные положения Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональнымиданными(23 сентября 1980 года) – Электронный ресурс – [Режим доступа] - http://online.zakon.kz/Document/?doc_id=31049166

8**DataProtectionAct 1998**– Электронный ресурс – [Режим доступа] - **https://www.legislation.gov.uk/ukpga/1998/36/contents**

9**FreedomofInformationAct 2000** – Электронный ресурс – [Режим доступа] - **https://www.legislation.gov.uk/ukpga/2000/29/contents**

10 Жарова А.К. Опыт правового обеспечения безопасности персональных данных в Великобритании // Государство и право. – 2017. -№6. –С.70-79

11 Родимцева М.Ю. Регулировать нельзя манипулировать // Государство и право. – 2016. - №7. –С.67-73

12 Сабитов Д. Информационная безопасность Казахстана: защита данных и смыслов.-Астана:ИМЭП, 2016. – 70с. – Электронный ресурс – [Режим доступа] - http://iwep.kz/files/attachments/article/2016-04-07/doklad_-sabitov.pdf

13Абраров Р. Д., Курязов Д. А. Информационная безопасность в компьютерных сетях // Молодой ученый. — 2016. — №9.5. — С. 10-12. — URL https://moluch.ru/archive/113/29719/.

14 Копылов В.А. Информационное право. –М.: Юрист, 2002. – 612с.

15 Шайхаттарова С.В. Россия и международные стандарты по борьбе с киберпреступностью // Международное уголовное право и международная юстиция. - 2016.- № 4. -С. 27.

16Конвенция об обеспечении международной информационной безопасности (концепция) – Электронный ресурс – [Режим доступа] -- http://www.scrf.gov.ru/documents/6/112.html

17 Протокол о взаимодействии государств-членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере, совершенный в Москве 23 декабря 2014 года. – Электронный ресурс – [Режим доступа] -- http://www.government.kz/images/zakony2016/11/rus/Z160000047620160328.

18 Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) - Электронный ресурс – Режим доступа -https://ccdcoe.org/sites/default/files/.../SCO-090616-IISAgreementRussian.pdf