УДК 341.01

ТЕНДЕНЦИИ РАЗВИТИЯ ИНСТИТУТА МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А. А. Ефремов

Воронежский государственный университет

Поступила в редакцию 12 сентября 2016 г.

Аннотация: *статья посвящена анализу современных тенденций развития международной информационной безопасности как института международного права.*
Ключевые слова: *информационная безопасность, международное право, международные организации.*

Abstract: *the article is devoted to analysis of modern trends of the development of international information security law as a institute of international law.*
Key words: *information security, international law, international organizations.*

В настоящее время вопросы регулирования информационной безопасности получают все большее развитие в рамках международного информационного права как отрасли международного права.

Данное регулирование складывается как из юридически обязательных норм международных договоров, так и из «мягкого права» – деклараций, рекомендаций и докладов органов международных организаций, – таких как ООН, ОЭСР, ШОС, ОДКБ и др.

Развитие международно-правового института международной информационной безопасности осуществляется в значительной мере по инициативе Российской Федерации как на уровне ООН, так и в рамках двухсторонних соглашений и документов таких международных организаций, как СНГ, ШОС, ОДКБ.

В рамках ООН в 1998 г. по инициативе Российской Федерации была принята резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[1] (A/RES/53/70), предусматривающая подготовку докладов Генерального секретаря ООН по данной теме, содержащих позиции государств – членов ООН по таким вопросам, как:

– общая оценка проблем информационной безопасности;

– усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

– содержание концепций (информационная безопасность, несанкционированное вмешательство, неправомерное использование);

– возможные меры, которые могли бы быть приняты международным

[1] Официальный сайт ООН. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 30.08.2016).

сообществом для укрепления информационной безопасности на глобальном уровне.

С 2010 г. Генеральным секретарем ООН представлялись доклады, содержавшие позиции государств по вопросам информационной безопасности (2010 г. – A/65/154; 2011 г. – A/66/152; 2013 г. – A/68/156; 2014 – A/69/112).

Кроме того, в период 2004–2015 гг. были созданы 4 группы правительственных экспертов, представлявшие свои доклады соответственно, на 60, 65, 68 и 70-й сессиях Генеральной ассамблеи ООН.

В данных докладах важное значение имеет обоснование взаимосвязи между обеспечением государственного суверенитета и международно-правовым регулированием информационных отношений.

В докладе, представленном на 68-й сессии Генеральной Ассамблеи ООН в 2013 г., указано, что государственный суверенитет и международные нормы и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории (п. 20)[2].

В докладе группы правительственных экспертов, представленной на 70-й сессии Генеральной Ассамблеи ООН в 2015 г.[3], данная группа предлагает государствам рассмотреть следующие рекомендации в отношении добровольных и необязательных норм, правил или принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды:

а) в соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности;

б) в случае инцидентов в сфере ИКТ государства должны изучить всю соответствующую информацию, в том числе более общий контекст события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий;

[2] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/68/98. Официальный сайт ООН. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R (дата обращения: 30.08.2016).

[3] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174. Официальный сайт ООН. URL: http://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement (дата обращения: 30.08.2016).

в) государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ;

г) государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. Государствам, возможно, потребуется рассмотреть вопрос о разработке новых мер в этой сфере;

д) в процессе обеспечения безопасного использования ИКТ государства должны соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете и резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение;

е) государство не должно осуществлять или заведомо поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит его обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения;

ж) государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции;

з) государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета;

и) государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование пагубных скрытых функций;

к) государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры;

л) государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группам готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

В отношении реализации государственного суверенитета в докладе отмечено, что суверенитет государств и международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с ИКТ, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территориях.

Согласно позиции Министерства иностранных дел РФ, итоговый доклад Группы является важным политико-правовым документом, закладывающим общие рамки для взаимодействия государств в информационном пространстве[4].

Развитие международно-правового института международной информационной безопасности в форме международно-правовых договоров в настоящее время осуществляется только в рамках отдельных международных организаций либо на двухстороннем уровне.

Например, согласно Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, утвержденной Решением Совета глав государств Содружества Независимых Государств от 10 октября 2008 г.[5], интересы государств – участников СНГ в информационной сфере заключаются в ее гармоничном формировании, наиболее эффективном развитии и использовании в целях реализации прав и свобод человека и общества, соблюдения норм законности и правопорядка, *обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности государств – участников СНГ*, достижения ими экономического роста, политической и социальной стабильности.

16 июня 2009 г. было подписано межправительственное Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, которое среди принципов закрепляет невмешательство в информационные ресурсы государств Сторон (ст. 4). Каждая Сторона имеет равное право на защиту информационных ресурсов и критически важных структур своего государства от неправомерного

[4] Об итогах заключительного заседания Группы правительственных экспертов ООН по международной информационной безопасности. Официальный сайт МИД России. URL: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1525144 (дата обращения: 30.08.2016).

[5] Интернет-портал СНГ. URL: http://www.e-cis.info/page.php?id=20229 (дата обращения: 30.08.2016).

использования и несанкционированного вмешательства, в том числе от информационных атак на них.

На уровне Российской Федерации в 2013 г. Президентом РФ были утверждены Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.[6]

Под международной информационной безопасностью в Основах понимается такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры.

Под системой международной информационной безопасности понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Система международной информационной безопасности призвана оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Согласно Основам, цель государственной политики Российской Федерации заключается в содействии установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности.

Согласно п. 17 Основ, государственная политика Российской Федерации реализуется федеральными органами исполнительной власти и надзорными органами в соответствии с предметами их ведения при выполнении соответствующих межгосударственных целевых программ, в осуществлении которых участвует Российская Федерация, государственных и федеральных целевых программ, в том числе в рамках государственно-частного партнерства.

Совет безопасности РФ осуществляет мониторинг реализации Основ. В частности, 3 февраля 2016 г. в Аппарате Совета безопасности РФ подведены итоги деятельности органов государственной власти, направленной на содействие формированию системы международной информационной безопасности[7].

20 ноября 2013 г. подписано Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности[8]. Данное соглашение не содержит

[6] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года : утв. Президентом РФ 24 июля 2013 г. № Пр-1753. Доступ из справ.-правовой системы «КонсультантПлюс».

[7] Совет безопасности РФ. Официальный сайт. URL: http://www.scrf.gov.ru/news/1020.html (дата обращения: 30.08.2016).

[8] Официальный интернет-портал правовой информации. URL: http://

положений о суверенитете государств и связи суверенитета и информационной безопасности.

Советом безопасности РФ разработана концепция универсальной Конвенции об обеспечении международной информационной безопасности[9].

Согласно данной концепции, политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств, и что государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня. Деятельность государств в информационном пространстве должна гарантировать свободу технологического обмена и свободу обмена информацией с учетом уважения суверенитета государств и их существующих политических, исторических и культурных особенностей.

Согласно концепции, в целях создания и поддержания атмосферы доверия в информационном пространстве необходимо соблюдение государствами следующих принципов:

– деятельность каждого государства-участника в информационном пространстве должна способствовать социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности, соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека;

– все государства-участники в информационном пространстве пользуются суверенным равенством, имеют одинаковые права и обязанности и являются равноправными субъектами информационного пространства независимо от различий экономического, социального, политического или иного характера;

– каждое государство вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства-участника или иным образом находящуюся под его юрисдикцией. Государства должны стремиться к гармонизации национальных законодательств, различия не должны создавать в них барьеры на пути формирования надежной и безопасной информационной среды;

– каждое государство, учитывая законные интересы безопасности других государств, может свободно и самостоятельно определять свои инте-

publication.pravo.gov.ru/Document/View/0001201506040007 (дата обращения: 30.08.2016).

[9] Конвенция об обеспечении международной информационной безопасности (концепция) // Совет Безопасности Российской Федерации. Официальный сайт. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 30.08.2016).

ресы обеспечения информационной безопасности на основе суверенного равенства, а также свободно выбирать способы обеспечения собственной информационной безопасности в соответствии с международным правом.

Концепция Конвенции оказала значительное влияние на подписание двухсторонних соглашений Российской Федерации в сфере международной информационной безопасности.

11 июля 2014 г. было подписано межправительственное Соглашение между Правительством РФ и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности. Соглашение относит к числу основных угроз международной информационной безопасности неправомерное использование информационных и коммуникационных технологий:

– в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на нарушение суверенитета, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

– для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической обстановки, нарушения управления государством и в целях свержения конституционного строя.

8 мая 2015 г. было подписано межправительственное Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности. Документ вступил в силу 10 августа 2016 г.

В преамбуле данного Соглашения подтверждается, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием информационно-коммуникационных технологий, и юрисдикцию государств над информационной инфраструктурой на их территории, а также то, что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью «Интернет», включая обеспечение безопасности.

Согласно Соглашению, первой среди основных угроз международной информационной безопасности является использование информационно-коммуникационных технологий для осуществления актов агрессии, направленных на нарушение суверенитета, безопасности, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

25 июня 2016 г. было подписано Совместное заявление Президента РФ и Председателя КНР о взаимодействии в области развития инфор-

мационного пространства[10]. Согласно данному заявлению, руководители двух стран поддерживают принцип уважения государственного суверенитета в информационном пространстве, рациональные требования всех стран по защите собственной безопасности и развитию, предлагают сформировать мирное, безопасное, открытое и основанное на сотрудничестве информационное пространство и разработать в рамках ООН универсальные правила ответственного поведения в информационном пространстве. Они выступают за равные права для всех государств на участие в управлении сетью «Интернет», а также признают право на защиту национальной безопасности в информационном пространстве с учетом практики законодательства и государственной системы, поддерживают инициативу создания многосторонней, демократичной, прозрачной системы управления сетью «Интернет» и важную роль ООН в вопросе создания международных механизмов управления Интернетом.

Как было указано выше, одним из ключевых элементов реализации государственного суверенитета в информационной сфере является осуществление юрисдикции в отношении ИКТ-инфраструктуры на территории данного государства, а двухсторонние соглашения в сфере международной информационной безопасности содержат специальные нормы об информационной инфраструктуре и о критически важных объектах.

Вместе с тем принимаемые в рамках международных организаций документы об обеспечении информационной безопасности в отношении информационной инфраструктуры содержат разные понятия.

Вышеуказанные соглашения с Республикой Кубой 2014 г. и Китайской Народной Республикой 2015 г. определяют информационную инфраструктуру как совокупность технических средств и систем создания, преобразования, передачи, использования и хранения информации, Соглашение ШОС 2009 г. – как совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации.

Соглашение с Китайской Народной Республикой 2015 г. содержит также понятие «критически важные объекты» – объекты инфраструктуры государства, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики государства либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на территории государства, на длительный срок. Соглашение ШОС 2009 г. содержит иное понятие – «критически важные структуры» – объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства.

[10] Совместное заявление Президента РФ и Председателя КНР о взаимодействии в области развития информационного пространства от 25 июня 2016 г. // Президент России. Официальный сайт. URL: http://www.kremlin.ru/supplement/5099 (дата обращения: 30.08.2016).

В рамках работы Межпарламентской ассамблеи СНГ 28 ноября 2014 г. приняты модельные законы «Об информации, информатизации и обеспечении информационной безопасности»[11] и «О критически важных объектах информационно-коммуникационной инфраструктуры»[12].

Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» содержит понятие *критически важная информационно-коммуникационная инфраструктура* – совокупность средств и систем формирования, создания, преобразования, передачи, использования и хранения информации, отказ или разрушение которых может оказать существенное отрицательное воздействие на национальную безопасность.

В свою очередь, модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры» содержит иные понятия:

информационно-коммуникационная инфраструктура – совокупность территориально распределенных государственных и корпоративных информационных систем, сетей связи, средств коммутации и управления информационными потоками, а также организационных структур и нормативно-правовых механизмов регулирования, обеспечивающих их эффективное функционирование;

критически важные инфраструктуры – объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьезный ущерб социальному, экономическому или политическому порядку или национальной безопасности;

критический элемент критически важного объекта информационно-коммуникационной инфраструктуры – структурный компонент критически важного объекта информационно-коммуникационной инфраструктуры, выход из строя которого с неизбежностью приводит к нарушению или прекращению функционирования объекта в целом;

объект информационно-коммуникационной инфраструктуры – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию.

В рамках Парламентской Ассамблеи Организации Договора о коллективной безопасности принят также ряд документов, содержащих различные понятия и их определения:

[11] Документы Межпарламентской Ассамблеи Содружества Независимых Государств. URL: http://iacis.ru/upload/iblock/25c/prilozhenie_k_postanovleniyu_15.pdf (дата обращения: 30.08.2016).

[12] Документы Межпарламентской Ассамблеи Содружества Независимых Государств. URL: http://iacis.ru/upload/iblock/f3b/prilozhenie_k_postanovleniyu_14.pdf (дата обращения: 30.08.2016).

– Рекомендации по гармонизации законодательства государств – членов ОДКБ в сфере обеспечения безопасности критически важных объектов от 27 ноября 2014 г. №7-5[13];

– Рекомендации по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности от 27 ноября 2014 г. №7-6[14].

Параллельно с процессами развития института международной информационной безопасности под эгидой ООН идет формирование института регулирования цифровой экономики и цифровой безопасности в рамках ОЭСР.

17 сентября 2015 г. Совет ОЭСР принял Рекомендацию и сопроводительный документ по управлению рисками цифровой безопасности для экономического и социального процветания (Digital security risk management for economic and social prosperity. OECD Recommendation and Companion Document. 17 September 2015 – C (2015) 115)[15].

Нацеливая государства на принятие стратегий цифровой безопасности, данная Рекомендация не содержит упоминаний о суверенитете государств в цифровом пространстве. Однако при этом неоднократно подчеркивается значимость вовлечения всех заинтересованных субъектов (англ. – *all stakeholders*), т.е. Рекомендация ориентирована на так называемое много-субъектное регулирование (англ. – *multistakeholder regulation*).

Концепцию «мультистейкхолдеризма» (англ. – *multistakeholderism*), отраженную в указанных положениях Рекомендации, следует определять именно как «многосубъектное регулирование» (англ. – *multistakeholder regulation*). Ее следует отличать от «многостороннего» (англ. – *multilateral*) регулирования (мультилатерализма). Ключевым отличием двух концепций является включение в число субъектов-регуляторов не только государств, но и граждан, бизнеса и институтов гражданского общества. Следует отметить, что противостояние двух подходов – мультистейкхолдерной модели, основанной на участии всех заинтересованных сторон, и мультилатеральной, которая отдает приоритет международной дипломатии и международным организациям, было рассмотрено 7 апреля 2016 г. на VII Российском форуме по управлению Интернетом. У. Дрейк (Университет Цюриха) высказал мнение, что эти две модели следует рас-

[13] Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: http://www.paodkb.ru/upload/iblock/917/rekomendatsii-po-garmonizatsii-zak_va-gos._chlenov-odkb-v-sfere-obespech.-bezop.-kritich.-vazhn.-obektov.pdf (дата обращения: 30.08.2016).

[14] Парламентская Ассамблея Организации Договора о коллективной безопасности. URL: http://www.paodkb.ru/upload/iblock/c07/rekomendatsii-po-sblizhen.-i-garmoniz.-natsion.-zak_va-gos._chlenov-odkb-v-sfere-obesp.-inf._kommunik.-bezop..pdf (дата обращения: 30.08.2016).

[15] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, 2015. 74 p.

сматривать не как взаимоисключающие, а как взаимодополняющие, а мультистейкхолдерной модели следует заимствовать у мультилатерализма более строгое следование законам и правилам[16].

Таким образом, анализ тенденций развития института международной информационной безопасности как элемента реализации государственного суверенитета позволяет сделать следующие выводы:

– формирование подходов к регулированию международной информационной безопасности на универсальном уровне идет в рамках рекомендаций группы правительственных экспертов ООН, носящих характер «мягкого права»;

– развитие российской модели международной информационной безопасности осуществляется в рамках двухсторонних соглашений, которые в перспективе могут являться основой для подписания многосторонних конвенций как на региональном уровне, так и в рамках ООН;

– необходима координация действий в рамках различных международных организаций, направленная на формирование и обеспечение единого международно-правового режима информационной безопасности на основе единого понятийного аппарата и принципов;

– параллельно с развитием института международной информационной безопасности осуществляется формирование института управления рисками цифровой безопасности при построении так называемой цифровой экономики. Данный институт в отличие от международной информационной безопасности ориентирован в значительной мере не на участие государств, а на «многосубъектное» регулирование.

[16] Разные модели управления Интернетом дополняют друг друга // Координационный центр национального домена сети «Интернет». URL: http://cctld.ru/ru/press_center/news/news_detail.php?ID=9661 (дата обращения: 30.08.2016).

Воронежский государственный университет

Ефремов А. А., кандидат юридических наук, доцент

E-mail: yefremov@law.vsu.ru

Voronezh State University

Efremov A. A., Candidate of Legal Sciences, Associate Professor

E-mail: yefremov@law.vsu.ru